# Hacker Highschool

## SECURITY AWARENESS FOR TEENS



# LESSON 4
# PLAYING WITH DAEMONS

နောက်ကွယ်မှ ဂန်ဆောင်မှုပရိုဂရမ်များဖြင့်

ကစားခြင်း

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM



WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

## သတိပေးချက်

ဤ Hacker Highschool စီမံကိန်း သည်၊ လေ့လာသင်ယူရေး ကရိယာ တစ်ခုဖြစ်ပြီး လေ့လာရေး အချက်များပါဂင်သည့်အလျောက် အနသတရာယ်ရှိပါသည်။ အကယ်၍ အချို့သောသင်ခန်းစာများအား၊ တလွဲအသုံး ချခြင်း၊ အဖျက်အမှောင့်ရည်ရွယ်ချက်ဖြင့်သုံးခြင်းသည်၊ ကိုယ်တိုင်နစ်နာမှုများဖြစ်စေနိုင်ပါသည်။ နည်းပညာအချက်အလက် များမှ ဖြစ်နိုင်ချေရှိသောရလာဒ်များကို သေချာစွာလေ့လာမထားပါက၊ ဘေးထွက်ဆိုးကျိုးများ ဖြစ်ပေါ်လာနိုင်ပါသည်။ ဤသင်ခန်းစာများကိုအသုံးပြုသော ကျောင်းသား၊ သူများသည်၊ လေ့လာခြင်း ၊ ကြိုးစားအားထုတ်ခြင်းနှင့် လက်တွေ့ အသုံးချခြင်းများ ပြုလုပ်ရာတွင် ကောင်းစွာသင်ကြားခြင်းများကို သင်ယူခြင်းအပြင်၊ စနစ်တကျ ကြီးကြပ်ခြင်းကို ခံယူသင့်ပါသည်။ မည်သို့ဖြစ်စေ ISECOM အဖွဲ့အစည်းမှ ဤသင်ခန်းစာများတွင်ပါဂင်သော မည်သည့်သတင်းအချက် အလက်များကိုမဆို လွဲမှားစွာအသုံးပြုခြင်းအတွက်တာဂန်ယူနိုင်မည် မဟုတ်ပါ။

အောက်ပါသင်ခန်းစာများ၊ လေ့ကျင့်ခန်း စာအုပ်များကို မည်သူမဆို ISECOM ၏စည်းကမ်းချက်များ အား လိုက်နာ၍ ဖတ်ရှုလေ့လာနိုင်ပါသည်။ ပုဂ္ဂလိကနည်းပညာကျောင်း၊ နိုင်ငံတော် နည်းပညာကျောင်းများ၊ အခြေခံ အလယ်တန်း၊အထက်တန်းများတွင် Hacker Highschool စီမံကိန်းမှ ဆောင်ရွက်မှုများ အားလုံးကို စီးပွားဖြစ်အသုံး ပြုခြင်းများအား တားမြစ်ပါသည်။ ဤစာအုပ်ပါ အချက်အလက်များအား ကူးယူ၍၊ မည်သည့် ပုံစံဖြင့်ဖြစ်စေ ပြန်လည် ထုတ်လုပ်ရောင်းချခြင်းများအား တားမြစ်ပါသည်။

ဤစာအုပ်ပါအချက်အလက်များမှမည်သည့်အမျိုးအစားဖြစ်စေ၊သင်ခန်းစာဖြစ်စေ (သို့)လေ့ကျင့်ခန်း များ ဖြစ်စေ ပါဂင်မှုများအား ခွင့်ပြုချက်လိုင်စင် မရှိပဲ တန်ဖိုးတစ်ခုခုဖြင့်ရောင်းချခြင်းကို ပြင်းထန်စွာတားမြစ်ထားပါ သည်။

လိုင်စင်ဂယ်ယူရန် http://www.hackerhighschool.org/licensing.html HHS website တွင်ဂယ်ယူနိုင်ပါသည်။ ဤ HHS စီမံကိန်းတွင် အဖိုးတန်မှု၊အကျိုးရှိမှုများ ရှိမည်ဆိုလျင်၊ HHS အား License ဂယ်ယူခြင်း၊ လူဒါန်းခြင်း၊အထောက်အပံ့ပေးခြင်းများ ဖြင့် ကူညီပေးပါရန် တောင်းဆိုပါသည်။

# Table of Contents

## Contributors

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Bob Monroe, ISECOM
Jaume Abella, ISECOM
Greg Playle, ISECOM
Simone Onofri, ISECOM
Guiomar Corral, Barcelona
Ashar Iqbal

## Translators

Htet Aung @ Starry Sky, Myanmar

ISECOM

## နိဒါန်း

လူအသိုင်းအဝိုင်းမှာ ကွဲပြားခြားနားတဲ့၊ ထောင်ပေါင်းများစွာသော ဘာသာစကားများစွာရှိပြီး ထိုဘာသာစကားအချို့ ကြားမှာ ဒါဇင်ပေါင်းများစွာသော ဒေသခံစကားများ များစွာရှိပါတယ်၊ ခင်ဗျားအနေနဲ့ ဘာသာစကားအချို့ကို ကိုယ်တိုင် ကိုယ်ကျ သိကောင်းသိပြီးသား ဖြစ်နိုင်ပေမယ့်၊ ကမဿဘာကို လှည့်လည်ခရီးသွားရင်း တွေ့သမသွားတိုင်း နှင့် စကားပြောနိုင်ရန် အလားအလာ ကတော့ မရှိသလောက်ကိုနည်းပါးတယ်။

သချာသငဇေဒက ကမဿဘာသုံးဘာသာစကားတစ်ခုဖြစ်တယ်ဆိုတာနှင့် ဂီတက လူတိုင်းကိုဆက်သွယ်နိုင်တယ်ဆိုတာ တွေကို စောဒကတက်နိုင်ပါတယ်၊ ဒါပေမယ့်လက်တွေ့ကျကြောရအောင်။ ဆိုဒါတစ်ခွက်ကို သံပရာ အနည်းငယ် နှင့် ရေခဲမုန့် ယောက်ချို့ တစ်ခပ်စာကို "ကမဿသဘာသုံး ဘာသာစကား" အသုံးပြုပြီး မှာယူခြင်းဖြင့် ဘယ်လောက်များများ ရနိုင်မယ်ဆိုတာစမ်းသပ် ကြည့်ပါ။

အကယ်၍ ခင်ဗျားမသိတဲ့ဘာသာစကားအသုံးပြုတဲ့ နိုင်ငံတစ်ခုမှာ ခင်ဗျားရှိနေတဲ့အခါ၊ ISECOM ဆီကို ဂီတတူရိယာ၊ လေမှုတ်တူရိယာ တစ်ခုခုဖြင့် ဆိုဒါတစ်ခွက်မှာယူနေတဲ့ ခင်ဗျားရဲ့ ဗွီဒီယိုဖိုင်တစ်ခုလောက် ပေးပို့လိုက်ပါ။ ကျွန်တော်တို့ တကယ်ကို ကြည့်ချင်ပါတယ်! ကျွန်တော်တို့ ကြားတော့မကြားချင်ပါဘူး ဒါပေမယ့် တကယ့်ကို မြင်ချင်ပါတယ်။

ဒါပေမယ့်၊ အင်တာနက်ပေါ်မှ သန်းပေါင်းများစွာသော လူတွေတိုင်းက တစ်ဦးနှင့်တစ်ဦးဆက်သွယ်နိုင်ရန် အတွက် ဘုံသုံးဖြစ်တဲ့ဘာသာစကား တစ်ခုတည်းကို အသုံးပြုကြပါတယ်။ လူတိုင်းကတော့ ဘာသာစကားတစ်ခုတည်းကို ပြောဆိုခြင်း မပြုနိုင်ပါဘူး၊ မည်သို့ဆိုစေ၊ ကျွန်တော်တို့ ကွန်ပြူတာများနှင့် ကွန်ယက်များကတော့ ဘာသာစကား တစ်ခုတည်းကိုပဲ ပြောကြပါတယ်။

> ခေတ်ပြိုင်ဖြစ်သောကွန်ယက်များကြားမှ ၁ ကျွန်တော်တို့အသုံးပြုနေကြတဲ့ ပုံစံဒီဇိုင်းက **ပန်ဆောင်မှုသုံးသူ-ပန်ဆောင်မှုပေးသူ (client-server)ဒီဇိုင်း** ပဲဖြစ်ပါတယ်။ ရူပဝိုင်းဆိုင်ရာ ကွန်ပြူတာများ **(host** သို့ **server)**များက (Unix စနစ်တွေမှ ၁ **daemons: disk access and execution monitors)** လို့ခေါ်တဲ့ **ပန်ဆောင်မှုများ**ကို လုပ်ဆောင်ပေးပါတယ်။ web server များကိုစဉ်းစားကြည့်ပါ။ ။ ၎င်းတို့က ခင်ဗျား web စာမျက်နှာ တစ်ခုကို ခေါ်လိုက်တိုင်း ပန်ဆောင်မှုများဆောင်ရွက်ပါတယ်။ ထွေထွေထူးထူးတော့ မဟုတ်ပါဘူး။

တစ်ကယ်တော့ "ခင်ဗျား"က အဲဒီ web စာမျက်နှာကိုခေါ်လိုက်တာ မဟုတ်ပါဘူး၊ ဒါပေမယ့် ခင်ဗျားရဲ့ web browser ကလုပ်ဆောင်ခြင်းပဲဖြစ်ပါတယ် ၎င်းကို **ပန်ဆောင်မှုတောင်းခံသူ client** (ပိုတိတိကျကျပြောရရင် ခင်ဗျားရဲ့ကွန်ပြူတာ) လို့ခေါ်ပါတယ်။ ပြီးတော့တစ်ချိန်တည်းမှာ၊ ခင်ဗျားကွန်ပြူတာကလည်း ပန်ဆောင်မှုပေးသူ (server) ဖြစ်နိုင်ပါတယ်။ ခင်ဗျားက ဒီအရာကို ကျွန်တော့်အတွက် ဆောင်ရွက်ပေးပါတယ်; ကျွန်တော်က ထိုအရာကို ခင်ဗျားအတွက် ဆောင်ရွက်ပေးပါတယ်၊ ဆိုတဲ့အချက်ကတော့ ကွန်ယက်ချိတ်ဆက်ခြင်းရဲ့ ဆန်းပြားလှပမှု တစ်ခုပါပဲ။

ဒီပုံစံကို အကြိမ်တစ်သန်းလောက်မြောက်လိုက်ရင် အင်တာနက်ဆိုတာ ရရှိလာပါလိမ့်မယ်။ ချင့်ချိန်ကြည့်ကြမယ်ဆိုရင်၊ ကွန်ပြူတာသန်းပေါင်းများစွာက ပန်ဆောင်မှုပုံစံအချို့ကို ဆောင်ရွက်နေကြပါတယ်၊ မည်သည့်အရာက ၎င်းကို client တစ်လုံး ဖြစ်စေတာလဲ? ပြီးတော့ ၎င်းစနစ်အားလုံးကို **subvert သွယ်ပို်က်စွာတိုက်ခိုက်**် ဖြိုဖျက်နိုင်သလား? ( subvert စကားလုံးအဓိပသယပါယ်ကို ခင်ဗျား တိကျစွာနားမလည်နိုင်ရင် သေချာရန် ရှာဖွေကြည့်ပါ). ယသသခုသင်ခန်းစာတွေက Hacker သင်ခန်းစာများဖြစ်ပါတယ်၊ အဆင်သင့်ဖြစ်ဖြစ်၊မဖြစ်ဖြစ် စတင်ကြရအောင်။

## ပန်ဆောင်မှုများ

ခင်ဗျားမှာကွန်ပြူတာတစ်လုံးရှိပြီးအဲဒီပေါ်မှာ အသုံးပင်တဲ့သတင်းအချက်အလက်တွေရှိနေတာခင်ဗျားသိပြီးဖြစ်မှာပါ သို့မဟုတ် ဂဏန်းတန်ဖိုးမရှိတဲ့ ယေဘူယျ အထင်မှားခြင်းအာရုံကြားမှာ ခင်ဗျားပါပင်နေတာလဲ ဖြစ်နိုင်ပါတယ်။ အခြားသန်း ပေါင်းများစွာသော လူတွေဆီမှာလည်း၊ အသုံးပင်တဲ့ အချက်အလက်တွေရှိတဲ့ ကွန်ပြူတာ တွေရှိတယ်ဆိုတာ ကိုလည်း ခင်ဗျားသိပါတယ်၊ processor, RAM, disk space နှင့် bandwidth စသည်ကဲ့သို့ အသုံးပင်တဲ့ အရင်းအမြစ်တွေကို ဖေါ်ပြရန်မဟုတ်ပါဘူး။

အဲဒီအခြားလူတွေနဲ့ ၎င်းတို့ရဲ့ကွန်ပြူတာတွေမှာ တစ်ယောက်ယောက်အတွက်စိတ်ပင်စားစရာ အချက်အလက်တွေ ရှိနေတယ်လို့ ယူဆကြည့်ပါ၊ တစ်ခုတည်းသောပြဿနာကာ အဲဒီအချက်အလက်တွေအားလုံးကို မည်သို့ရယူနိုင်သလဲဆိုတဲ့ အချက်ပါပဲ။

ကွန်ပြူတာတွေက တစ်လုံးနှင့်တစ်လုံးချိတ်ဆက်ရန် ports များကိုဖြတ်သန်း၍၊ ကျွန်တော်တို့ Lesson 3 မှာ ဆွေးနွေးခဲ့ကြတဲ့ protocols များကိုအသုံးပြု၍ လွယ်ကူစွာ ဆက်သွယ်ကြပေမယ့်၊ ထိုကဲ့သို့ချိတ်ဆက်ခြင်းက ခင်ဗျားကို ၎င်းတို့ အချင်းချင်း ဖလှယ်ကြတဲ့ အခြေ့ တန်ဖိုးရှိ အချက်အလက်များ (binary data) တွေရဲ့ စီးဆင်းမှုတွေကို လွယ်ကူစွာဖတ်ရှုခွင့်မပြုပါဘူး (ခင်ဗျားလက်ထဲမှာ တကယ့်အရေးပါတဲ့အချိန်ပိုမရှိဘူးဆိုရင်ပေါ့)၊ ခင်ဗျားကွန်ပြူတာအတွက် ထိုအချက်အလက်တွေကို ရယူနိုင်ရန် ဘာသာပြန်ဆိုပြီး ခင်ဗျားသုံးနိုင်မည့်ပုံစံဖြင့် ဖေါ်ပြပေးနိုင်တဲ့ နည်းလမ်းတစ်ခုတော့ ခင်ဗျားအတွက် လိုပါတယ်။

အချက်အလက်ပေးပို့ရန် ကွန်ပြူတာများအသုံးပြုတဲ့နည်းလမ်းကတော့ **network service များ** သို့မဟုတ် သမရိုးကျ ပန်ဆောင်မှုများကို ဖြတ်သန်းသွ၍ပေးပို့ခြင်းပဲ ဖြစ်ပါတယ်။ ၎င်းပန်ဆောင်မှုများက ခင်ဗျားကို web စာမျက်နှာများကြည့်ရှုရန်၊ email များ ပို့ဆောင်ရန်, chatting နှင့် အပေးထိန်းကွန်ပြူတာများဖြင့် အပြန်အလှန်ချိတ်ဆက်မှုပြုရန်အတွက် ပန်ဆောင်မှုများ ဆောင်ရွက်ပေးပါတယ်။ ၎င်းပန်ဆောင်မှုများကို port နံပါတ်များဖြင့် ချိတ်ဆက်ရည်ညွှန်းထားပါတယ်။

ခင်ဗျားရဲ့ကွန်ပြူတာ၊ **local ကွန်ပြူတာ**ပေါ့ ၎င်းက ခင်ဗျားရရှိလာတဲ့အချက်အလက်တွေကို ဘာသာပြန်ဆိုရန်အတွက် **clients** လို့ခေါ်တဲ့ပရိုဂရမ်တွေကို အသုံးပြုပါတယ်။ **server** တစ်လုံးထံမှ အချက်အလက် တွေကို (ပန်ဆောင်မှုတစ်ခု ထောက်ပံ့ခြင်း သို့ daemon တစ်ခု မောင်းနှင်ခြင်းဖြင့်) **Tor** ကွန်ယက်တစ်ခုပေါ်မှ၊ **Torrent seeder** များမှ (သို့) **peer-to-peer** ကွန်ယက်များမှတဆင့် ခင်ဗျားရယူနိုင်ပါတယ်။

> ခင်ဗျားကွန်ပြူတာကလည်း အခြား remote ကွန်ပြူတာများကို ပန်ဆောင်မှုများဆောင်ရွက်ပေးနိုင်ပါတယ်၊ ဆိုလိုတာက ၎င်းက အချက်အလက်ပန်ဆောင်မှုပေးသူ (သို့) ပန်ဆောင်မှုထောက်ပံ့ပေးသူ တစ်ခုလည်း ဖြစ်နိုင်ပါတယ်။ အကယ်၍ ခင်ဗျားကွန်ပြူတာမှာ malware ရှိလာခဲ့ရင်တော့၊ ခင်ဗျားကိုယ်တိုင်မသိပဲပန်ဆောင်မှုအချို့ကို ထောက်ပံ့ပေးနေပါလိမ့်မယ်။

Client ဥပမာတွေကတော့ web browsers၊ email clients၊ chat ပရိုဂရမ်များ၊ Skype၊ Tor clients၊ Torrent clients၊ RSS များ စသည်တို့ဖြစ်ပါတယ်။ ၎င်းတို့ကတော့ TCP/IP protocol အဆင့်များတွင် **application အလွှာ**မှ application များဖြစ်ကြပါတယ်။ application အလွှာမှာ၊ ထုတ်ပိုးခြင်း၊ encrypt လုပ်ထားခြင်း၊ decrypt လုပ်ထားခြင်း၊ လိပ်စာတပ်ထားခြင်း စသည်ဖြင့် အတွင်းကျသောအလွှာများဖြင့် အဆင့်ဆင့် သယ်ယူပို့ဆောင်ထားသော အချက်အလက်များအားလုံးကို ခင်ဗျား၊ (အသုံးပြုသူ) အနေနဲ့ နားလည်နိုင်တဲ့ အနေအထားတစ်ခုခုအဖြစ် ပြန်လည်ပြောင်းလဲပေးပါတယ်။

### HTTP နှင့် Web

ကျွန်တော်တို့ "အင်တာနက်" လို့ပြောလိုက်တာနှင့် လူအများစုက **World Wide Web** ကိုပြေးမြင်ကြပါတယ်။ အဲဒီ World Wide Web (သို့) **Web** က အမှန်တကယ် အင်တာနက်မဟုတ်ပါဘူး၊ ၎င်းက အသုံးပြုနိုင်တဲ့ ပန်ဆောင်မှုတွေရဲ့ အစိတ်အပိုင်းတစ်ခုမျှသာဖြစ်ပါတယ်။ ပုံမှန်အားဖြင့်၎င်းက browser ကိုဖြတ်၍ web စာမျက်နှာ တွေကြည့်ရှုရာမှာ ပါဝင်ပါတယ်။

စကားမစပ်၊ တကယ့်အင်တာနက်မှာ၊ အချက်အလက် အမျိုးအစားမရွေး ရွှေ့ပြောင်းပို့ဆောင်နိုင်တဲ့ ကွန်ပြူတာများ၊ router များ၊ ဂါယာများ၊ ကြိုးများနှင့် ကြိုးမဲ့စနစ်များ ပါဂင်ပါတယ်။ web လမ်းကြောင်း ဆိုတာတွေရဲ့ အပိုင်းကိန်းမျှသာ ဖြစ်ပါတယ်။

Web တွေကို **web server များ**ပေါ်မှ အချက်အလက်များကို ရယူအသုံးပြုရန်အတွက် **HTTP** (သို့) **HyperText Transfer Protocol web browsers** လို့ခေါ်တဲ့ application (client) တွေကို အသုံးပြုပါတယ်။ remote ကွန်ပြူတာ ပေါ်မှ အချက်အလက်များကို ခင်ဗျားရဲ့ local ကွန်ပြူတာပေါ် ရွှေ့ပြောင်းပို့ဆောင်ရန်၊ ပုံမှန်အားဖြင့် HTTP protocol ကို port 80 ပေါ်မှာ အသုံးပြုပါတယ်။ ခင်ဗျားရဲ့ web browser က အဲဒီ အချက်အလက်ကို ဘာသာပြန်ပြီး ခင်ဗျားရဲ့ local ကွန်ပြူတာ ပေါ်မှာ စုစည်းတင်ပြပါတယ်။

browser အားလုံးကို တူညီစွာထုတ်လုပ်ထားတာမဟုတ်ပါဘူး။ တစ်ခုချင်းစီမှာ မတူညီတဲ့ tool တွေပါဂင်ပြီး HTML ပါဂင်မှုတွေကို အနည်းငယ် (သို့) များစွာ ခြားနားတဲ့ နည်းလမ်းများဖြင့် ထုတ်ဖော်ပြသပါတယ်။ လုံခြုံရေး နှင့် သီးသန့်တည်ရှိမှု ကိစ္စသစရပ်တွေကို သက်ရောက်မှုအတိုင်းအတာအမျိုးမျိုးဖြင့် ကိုင်တွယ်ဖြေရှင်းနိုင်ပါတယ်။ ဆိုလိုချင် တာက ခင်ဗျားbrowser က ဘာတွေ လုပ်ဆောင်နိုင်တယ်၊ ဘာတွေမလုပ်ဆောင်နိုင်ဘူး၊ မည်ကဲ့သို့သော setting များနှင့် plugins များက ပြီးပြည့်စုံတဲ့ လုံခြုံရေးနှင့် သီးသန့်တည်ရှိမှုတွေ (ခင်ဗျားက malware တွေ၊ ကြော်ငြာ တွေ၊ spam တွေကို မကြိုက်ဘူးဆိုရင် ပြီးတော့ ခင်ဗျားက အစိမ်းရောင်ဂျယ်လီတွေနဲ့ ဆော့ကစား နေတဲ့ ကြောင်လေးတွေကို ကြည့်နေရတာနှစ်သက်ကြောင်း ခင်ဗျား အိမ်နီးချင်းကမသိဘူးဆိုရင်) ကို ပေးစွမ်းနိုင်သလဲ ဆိုတာတွေကို ခင်ဗျားကိုယ်တိုင်သိထားသင့်ပါတယ်။

Http protocol ၏ အစိတ်အပိုင်းဖြစ်တဲ့ **hypertext** က ခင်ဗျားဖတ်ရှုတဲ့နည်းလမ်းကဲ့သို့ အစဉ်လိုက်မဟုတ်ပါဘူး။ ပုံမှန်အားဖြင့် ခင်ဗျားက စာမျက်နှာ ၁ ပြီးတော့ ၂၊ အခန်း ၁ ပြီးတော့ ၂၊ လေ့ကျင့်ခန်း ၁ ပြီးတော့ ၂ စသည်ဖြင့် အစဉ်အလိုက်ပုံစံအတိုင်း ဖတ်ရှုပါတယ်။ Hypertext က သတင်းအချက်အလက်များကို အစဉ်လိုက်မဟုတ်တဲ့ နည်းလမ်းဖြင့်ဖတ်ရှုနိုင်ရန် လုပ်ဆောင်ပေးပါတယ်။ ၎င်းက အကြောင်းအရာ တစ်ခုမှ၊ တစ်ခုသို့ ကျော်၍ပြန်လှန်၍ ဖတ်ရှုနိုင်ပြီး ခင်ဗျားဖြတ်သန်းခဲ့တဲ့လမ်းကြောင်းများကိုပြန်သွားခြင်း နှင့် မှရင်းဆောင်းပါးမပြီးခင်၊ အခြား အချက်အလက်များ ရှာဖွေ ဖတ်ရှုခြင်း စသည်တို့ကို လုပ်ဆောင်နိုင်ပါတယ်။ ဤအချက်က hypertext နှင့် plain text တို့၏ ကွာခြားချက်ပဲဖြစ်ပါတယ်။

Hypertext မှာ၊ စကားလုံးများ နှင့် စိတ်ကူးများကို ၎င်းတို့နှင့် တိုက်ရိုက်ဆက်နွယ်သောဂန်းကျင်ရှိစကားလုံးများဖြင့် ချိတ်ဆက်ခြင်းသာမက၊ အခြားစကားလုံးများ၊ ရုပ်ပုံများ၊ ဗွီဒီယိုများ၊ သီချင်းများဖြင့် လည်းချိတ်ဆက်ထားပါ တယ်။ Web ကို ရောက်ရှိရန် Hypertext ကိုမတားဆီးထားပါဘူး။ စွမ်းဆောင်ရည်ပြည့်ဂသော word processors အများစုကတော့ web ပေါ်မှာသိမ်းဆည်းထားတဲ့ စာမျက်နှာများ (သို့) HTML ပုံစံများကို ဖန်တီးနိုင်ပါတယ်။ ဤစာမျက်နှာများကို ခင်ဗျား web browser မှာဖတ်ရှုနေတာဖြစ်ပြီး ၎င်းတို့က အခြား web စာမျက်နှာ များကဲ့သို့ လုပ်ဆောင်ပါတယ်၊ ၎င်းတို့ကို remote ကွန်ပြူတာပေါ်မှာမဟုတ်ပဲ ခင်ဗျားရဲ့ local ကွန်ပြူတာပေါ်မှာပဲ သိမ်းဆည်းထားတာပါ။

ခင်ဗျားကိုယ်ပိုင် web စာမျက်နှာတစ်ခုဖန်တီးဖို့က လွယ်ပါတယ်။ အလွယ်ကူဆုံး နည်းလမ်းကတော့ OpenOffice/ LibreOffice Writer၊ Microsoft Word (သို့) Word Perfect ကဲ့သို့ ယေဘူယျ word processors တစ်ခုခု အသုံးပြုခြင်းပဲဖြစ်ပါတယ်။ ဤပရိုဂရမ်များဖြင့် ရိုးရှင်းသော web စာမျက်နှာများ၊ text များ၊ hypertex နှင့် ပုံများ ဖွဲ့စည်းမှုများ ထုတ်လုပ်နိုင်ပါတယ်။ လူတော်တော်များများက ၎င်းပရိုဂရမ်များကို အသုံးပြု၍ ( သို့မဟုတ်၊ Unix platforms များမှာပါလေ့ရှိတဲ့၊ vi ကဲ့သို့ ရိုးရှင်းသော text editor များကို အသုံးပြု၍ ) web စာမျက်နှာများကို တည်ဆောက်ခဲ့ကြပါတယ်။ အခြား text editor များ ဖြစ်ကြတဲ့ Microsoft Notepad, Notepad++, SciTe, emacs စသည့် text editor များကိုလည်းအသုံးပြုနိုင်ပါတယ်။

ဒါပေမယ့် ၎င်းစာမျက်နှာများက flashy မဟုတ်ကြပါဘူး။ Flashy ဆိုတာက **CSS**, **script** များနှင့် animations တွေကို ဆိုလိုတာပါ။ ခင်ဗျားအနေနဲ့ နှစ်သက်ချင်စရာ web စာမျက်နှာဒီဇိုင်း ပရိုဂရမ်များကို ပိုက်ဆံများများသုံးပြီး ဂယ်ယူနိုင်ပါတယ်။ ထိုဂရိုဂရမ်များက စိတ်ဂင်စားစရာ effect များ ဖန်တီးနိုင်ပေမယ့် အသုံးပြုဖို့တော့ ပိုမိုရှုပ်ထွေးပြီး၊ လုပ်ငန်းတစ်ခုလုံးကိုတော့ ပိုမိုလွယ်ကူစေပါတယ်။ ပြောင်းပြန်ဖြစ်တဲ့ ကုန်ကျစရိတ်သက်သာသော နည်းလမ်း တစ်ခုကတော့ HTML နှင့် scripting language များဖြင့်အသုံးပြုနိုင်တဲ့ သီးသန့်ပုံစံချထားတဲ့ Text Editor တစ်ခုခုကို သုံးနိုင်ရန်ဖြစ်ပြီး၊ HTML နှင့် scripting

များတည်ဆောက်မှုပုံစံကို လေ့လာသင်ယူပြီး ခင်ဗျားကိုယ်ပိုင် web စာမျက်နှာများကို အကြမ်းရေးခြစ်ထားခြင်းမှ coding များအဖြစ်အကောင်အထည်ဖော်ရေးသားပါ။

ခင်ဗျား web စာမျက်နှာတွေကိုပုံစံချပြီးတာနဲ့ ထိုစာမျက်နှာတွေကို အခြားလူတွေကိုလည်း မြင်စေချင်မယ်ဆိုရင် ၎င်းစာမျက်နှာများကို ထည့်သွင်းသိမ်းဆည်းထားရန် ကွန်ပြူတာတစ်လုံး လိုအပ်ပါလိမ့်မယ့်။ **Internet Service Providers (ISPs)** တွေက ၎င်းတို့ web server များပေါ်မှာ **web hosting** ဂန်ဆောင်မှုများကို ဆောင်ရွက် ပေးပါတယ်။

ခင်ဗျားကွန်ပြူတာကိုအသုံးပြုပြီး ခင်ဗျားအိမ်ကနေ web server တစ်ခုကို လုပ်ဆောင်စေနိုင်ပေမယ့်၊ ထိုသို့ လုပ်ဆောင်နိုင်ရန် များပြားတဲ့ကိစ္စသစရပ်တွေရှိပါတယ်။ web server တစ်လုံးပေါ်မှာ သိမ်းဆည်းထားတဲ့ အချက်အလက်တွေက အဲဒီ server ဖွင့်ထားတဲ့အချိန်၊ ကောင်းမွန်စွာလည်ပတ်နေတဲ့အချိန်နှင့် ချိတ်ဆက်မှု တည်ရှိနေတဲ့ အချိန်များမှာသာ ရယူအသုံးပြုနိုင်ပါတယ်။ ဒါကြောင့် ခင်ဗျားအိပ်ခန်းထဲကနေ web server တစ်လုံးကို လုပ်ငန်းဆောင်ရွက်စေမယ်ဆိုရင်တော့၊ ခင်ဗျားကွန်ပြူတာကို အချိန်တိုင်းဖွင့်ထားဖို့လိုအပ်ပြီး၊ web server ပရိဂရမ်က ကောင်းမွန်စွာ လုပ်ငန်းဆောင်ရွက်နေခဲ့လား (ဤအချက်မှာ စက်ပစ္စည်း ပြင်ဆင်ထိန်းသိမ်းခြင်း၊ ဗိုင်းရပ်(စ်) ပြဿနာများဖြေရှင်းခြင်း နှင့် အခြားတိုက်ခိုက်မှုများ စောင့်ကြည့် ထိန်းသိမ်းခြင်း၊ ၎င်း web server ပရိုရဂရမ်ခဲ့ မရှိမဖြစ်လိုအပ်သော အများအယွင်းများနှင့် အားနည်းချက် ပြဿနာများ ကိုင် တွယ်ဖြေရှင်းခြင်းများ ပါဝင်ပါတယ်။) ဆိုတာအချိန်တိုင်းစောင့်ကြည့်ဖို့ လိုအပ်ပါတယ်၊ ထို့အပြင် မြန်ဆန်ပြီးတည်ငြိမ်တဲ့ အင်တာနက်ချိတ်ဆက်မှုကိုလည်း အပြည့်အဝချိတ်ဆက်ထားရန်လိုအပ်ပါတယ်။ ISP များကတော့ မြန်ဆန်တဲ့ upload ချိတ် ဆက်မှုလိုင်း နှင့် IP လိပ်စာ သီးသန့်သတ်မှတ်ထားရှိမှုတို့ အတွက် ဂန်ဆောင်မှုအခကြေးငွေအား ထပ်ဆောင်း ကောက်ခံ ကြပါ တယ်၊ ထို့ကြောင့် လူအများစုက web server လုပ်ငန်းများလုပ်ဆောင်ရန်အတွက် web server ဂန်ဆောင်မှုပေးသူ တစ်ဦးဦး အား အခကြေးငွေပေး၍ အပ်နှံလုပ်ဆောင်ကြပါတယ်။

web hosting ကုမဿပဏီတစ်ခုက ခင်ဗျားရဲ့ web စာမျက်နှာအား ၎င်းတို့၏ကွန်ပြူတာပေါ်မှာ သိမ်းဆည်းကြပါတယ်။ ထိုအချက် က ခင်ဗျားကွန်ပြူတာအစား သူတို့ရဲ့ server များကိုတိုက်ခိုက်ခံရစေနိုင်ပါတယ်။ web hosting ကုမဿပဏီကောင်း တစ်ခုမှာ စက်ပစ္စည်းချွတ်ယွင်းချက်ကြောင့် ခင်ဗျား website ပျောက်ကွယ်မသွားစေရန်၊ ဆင့်ပွားချိတ်ဆက်ထားသော (multiple)၊ အချိန်မီအစားထိုးရန် အရံထားရှိသော (redundant) server များနှင့် အစဉ်မပြတ် backup ပေါ်လစီတစ်ခု အမြဲရှိပြီး၊ အကယ်၍ တိုက်ခိုက်မှုများနှင့် ပရိဂရမ်မှားယွင်းမှုများ ရှိနေခဲ့ရင်သော်လည်း server များကို ဆက်လက်လည်ပတ်နိုင်စေရန် အထောက် ကူပေးဂန်ထမ်းတစ်ယောက် ကလည်း အစဉ်မပြတ်ဂန်ဆောင်မှုပေးနေပြီး၊ အင်တာနက်လိုင်းကျခြင်း မရှိစေရန် အာမခံရှိသော၊ များစွာသော အင်တာနက် ချိတ်ဆက်မှုလိုင်းများလည်း ရှိပါလိမ့်မယ့်။ ဒါကြောင့် ခင်ဗျားအနေနဲ့ လုပ်စရာရှိတာကတော့ ခင်ဗျား web page ဒီဇိုင်းကိုပြင်ဆင်မြှင့်တင်ဖို့နှင့် hosting ကုမဿပဏီ၏ server ဆီသို့ upload လုပ်ဖို့၊ ပြီးတော့ ခင်ဗျားကွန်ပြူတာကို ပိတ်ပြီး အိပ်ယုံပါပဲ။ ခင်ဗျား ဂန်ဆောင်ခပေးနေသမျှတော့ ခင်ဗျား web စာမျက်နှာက ရှင်သန်နေပါလိမ့်မယ်။

အခမဲ့ web hosting ဂန်ဆောင်မှုပေးတဲ့ အဖွဲ့အစည်းတွေကိုလည်းရှာဖွေနိုင်ပါတယ်။ အချို့ အဖွဲ့အစည်းတွေက ကြော်ငြာ ရံပုံငွေဖြင့် ရပ်တည်နေကြတာပါ၊ အဲဒီ အခမဲ့ web hosting တွေကိုအသုံးပြုရင် ခင်ဗျားစာမျက်နှာကို ကြည့်တဲ့လူတိုင်းက၊ ခင်ဗျားစာမျက်နှာကိုဧရိယိုက်တိုင်း ပထမဦးစွာ ကြော်ငြာတစ်ခုခုကိုအရင်ဆုံးမြင်ရမှာဖြစ်ပါတယ်။ ဒါပေမယ့် သူတို့ကလဲ ဘာမျှ ဂယ်ယူဖို့မလိုသလို၊ ခင်ဗျားအနေနဲ့လည်း မည်သည့်အရာမျှ ပေးဖို့မလိုပါဘူး။

**လေ့ကျင့်ခန်းများ**

4.1 web စာမျက်နှာဆိုတာ ရုပ်ပုံတွေ၊ ဗွီဒီယိုတွေနှင့် အခြားအရာတွေဘယ်မှာရှိသင့်တယ်ဆိုတာ browser ကိုပြောတဲ့ text သာဖြစ်ပါတယ်။ စာမျက်နှာရဲ့ရင်းမြစ် ကိုကြည့်ရင် (View Page Source) ခင်ဗျားမြင်နိုင်ပါတယ်။ ခင်ဗျား အနှစ်သက်ဆုံး browser ကိုသုံးပါ၊ ISECOM.ORG ကိုညွှန်းကြည့်ပါ။ အခု page source ကိုကြည့်ပါ။ အဲဒီထဲမှာ "meta"ဆိုတဲ့ tags တွေကိုမြင်ပါလိမ့်မယ် ဥပမာ။ ။ meta-charset="utf-8"။ အဲဒါဘာကိုဆိုလိုပါသလဲ၊ ဘာကို ညွှန်ပြပါသလဲ?

4.2 Meta tag ဥခုလောက်ထပ်ရှာပါ ပြီးတော့ ၎င်းတို့ရဲ့ ရည်ရွယ်ချက်ကို ရှင်းလင်းပြပါ။ ထိုအချက်ကိုသိရန် web မှာ ရှာဖွေရန်လိုအပ်လာပါလိမ့်မယ်၊ ဒါကြောင့် အဖြေမှန်ရနိုင်ရန် ဘယ် key word တွေကိုသုံးပြီး ခင်ဗျား search engine မှာရှာဖွေမယ်ဆိုတာ သေချာစဉ်းစားပါ။

4.3 ISECOM.ORG page source ကို ခင်ဗျားကွန်ပြူတာပေါ်မှာ save ပါ။ ၎င်းကို ခင်ဗျား browserပေါ်ကို ဆွဲတင်ကြည့်ပါ၊ ဘာတွေပြောင်းလဲသွားသလဲ?

4.4 ISECOM.ORG page source ကို text editor တစ်ခုခုထဲမှာ ဖွင့်ကြည့်ပါ၊ ၎င်းက စာလုံးတွေနဲ့ နံပါတ်တွေ ဆိုတာ မြင်ရပါလိမ့်မယ်။ အဲဒီထဲမှာ ခင်ဗျားဘာပဲပြင်ပြင်၊ ဘာပဲရိုက်ရိုက် ပြင်ဆင်ပြီး အဲဒါကို save ပြီး browser မှာပြန် ဖွင့်ကြည့်ရင် ခင်ဗျားပြင်ဆင်ထားတဲ့အတိုင်း အဲဒီစာမျက်နှာမှာ ပြောင်းလဲသွားပါလိမ့်မယ်။ အခု အဲဒီစာမျက်နှာမှာ ရှိသမျှအားလုံးကို ဖျက်လိုက်ပြီး ခင်ဗျားနာမည် ရိုက်ထည့်လိုက်ပါ ၎င်းက အခြားစာလုံးတွေထက် ကြီးပြီး၊ ထူတဲ့ စာလုံးနဲ့ဖော်ပြပါလိမ့်မယ်။ save လုပ်ပြီး၊ browser မှာပြန်ဖွင့်ကြည့်ပါ။ အောင်မြင်သလားကြည့်ပါ၊ မရသေးရင် ထပ်ကြိုးစားကြည့်ပါ။

> ပိုမိုသိရှိနားလည်နိုင်ရန် ဒီသင်ခန်းစာအဆုံးမှာ ***Feed Your Head: HTTP နှင့်ကစားခြင်း*** ကိုလေ့လာကြည့်ပါ။

## Email – SMTP, POP and IMAP

အင်တာနက်ရဲ့ ဒုတိယ မြင်သာတဲ့ဖော်ပြချက်ကတော့ email ပဲဖြစ်ပါတယ်။ ခင်ဗျားကွန်ပြူတာမှာ (စာပို့၊စာယူ စနစ်အား ဝန်ဆောင်မှုပေးသူ) mail server ကိုချိတ်ဆက်နိုင်တဲ့ email client တစ်ခုကိုအသုံးပြုထားပါတယ်။ ခင်ဗျား email account တစ်ခု setup လုပ်လိုက်ရင် ပုံစံတူမရှိတဲ့နာမည် တစ်ခုကို **user@domain** ပုံစံနဲ့ ရရှိမှာဖြစ်ပြီး၊ စကားဝှက်တစ်ခု ပေးဖို့လည်း လိုပါလိမ့်မယ်။

> Email မှာအစိတ်အပိုင်း ၂ခု ရှိပါတယ်၊ စာပို့ရန်သုံးတဲ့ **SMTP(Simple Mail Transfer Protocol)**၊ mail server ပြီးတော့ mail လက်ခံရန်သုံးတဲ့ **POP(Post Office Protocol)** နှင့် **IMAP (Internet Message Access Protocol)** တို့ဖြစ်ကြပါတယ်။

SMTP protocol ကို (ခင်ဗျားကို သတိထပ်ပေးပါမယ်) email ပို့ရန်အသုံးပြုပါတယ်။ SMTP က email စာတစ်စောင်ထဲက (FROM)-မှ၊ (TO)-သို့၊ (SUBJECT)-အကြောင်းအရာ၊ (CC)-မိတ္တူသတူကို နှင့် (BODY)-စာကိုယ် များပါဝင်သည့် **fields-အကွက်များ** ကို သတ်မှတ်ပေးပါတယ်။ ရိုးရှင်းသော SMTP ပုံစံဟောင်းတွေကတော့ ပို့တဲ့စာတိုင်းကို ရှင်းလင်းတဲ့ စာသားပုံစံဖြင့် ပို့ဆောင်ပြီး၊ စကားဝှက်လည်းမလိုတာကြောင့် လူတိုင်းက ခင်ဗျားစာတွေကို ဖွင့်ဖတ်နိုင်ပါတယ်။ စိတ်သဘောတိုက်ဆိုင်တဲ့ လူတွေက အင်တာနက်ကို ကမ္ဘာဘင်္ဂလိတစ်ခုလိုအခြေချပြီး ၎င်း SMTP protocol ကိုပုံစံချခဲ့ကြတုန်းက ဤအချက် က ဆိုးဝါးမှုမရှိခဲ့ပါဘူး။ ဒါပေမယ့် ၎င်းက အသုံးပြုသူတိုင်းကို **spam** ပို့ခြင်း၊ အခြေခံအားဖြင့် လိပ်စာများပို့ခြင်း (spoofing) အပေါ်အခြေခံတဲ့ **email spoofing** များကဲ့သို့ ညစ်ပတ်မှုများ ပြုလုပ်ခွင့်ပေးတဲ့၊ loophole (စနစ်တစ်ခု၏ ချွတ်ယွင်းချက်၊ အားနည်းချက် နှင့် ရှုပ်ထွေးမှု) တစ်ခုကို ဖြစ်ပေါ်စေပါတယ်။ ခေတ်ပြိုင်ဖြစ်လာသော Mail Server များကတော့ email စာတစ်စောင်မပို့ခင် ခင်ဗျားမည်သူဖြစ်ကြောင်းအထောက်အထားပြရန်လိုတဲ့ လုံခြုံရေးဦစားပေး SMTP (Secure SMTP) ကို အသုံးပြုကြပါတယ်။

နောက်ပိုင်းသင်ခန်းစာများမှာ spoofing မည့်ကဲ့သို့ အလုပ်လုပ်တယ် ၎င်းကို email header များမှာ မည်သို့ရှာဖွေနိုင်တယ် ဆိုတာကို ဖော်ပြပေးမှာပါ။ ထိုအချက်က ခင်ဗျားကို သိုးငယ်တစ်ကောင်ကနေ ဝံပုလွေတစ်ကောင်ဖြစ်လာအောင် အမြန်ဆုံး ပြောင်းလဲပေးမယ့် အနည်းငယ်သောဗဟုသုတ ဖြစ်ပါတယ်။

**POP3 (Post Office Protocol version 3)** ကတော့ "ထိန်းသိမ်းခြင်း (store) နှင့် သိမ်းဆည်းခြင်း (dump)" protocol တစ်ခုပါ။ email server က ခင်ဗျား စာတွေကို လက်ခံထားပြီး ခင်ဗျားက ချိတ်ဆက် သိမ်းဆည်းမှု (dump-download) ပြုလုပ်သည်အထိ ၎င်းစာတွေကို ထိန်းသိမ်းထားပါတယ်။ ပြီးတော့၊ ခင်ဗျား ပို့လိုက်တဲ့စာတွေက SMTP protocol ကို အသုံးပြုပါတယ်၊ ခင်ဗျား email စာပို့ခြင်း၊ ရယူခြင်းကို အချိန်အနည်းငယ်အတွင်းပြုလုပ်နိုင်ပြီး၊ အင်တာနက်ချိတ်ဆက်မှုပိတ်ပြီး အဲဒီ email တွေကို ဖတ်နိုင်တာကြောင့်၊ ခင်ဗျားမှာ dail-up ချိတ်ဆက်မှုရှိယုံမျှဖြင့် email ဝန်ဆောင်မှုကို အသုံးပြုနိုင်ပါတယ်၊

**IMAP** ကတော့ ပုံမှန်အားဖြင့် ခင်ဗျားစာတွေကို server ပေါ်မှာထိန်းသိမ်းထားပေးတဲ့ protocol ဖြစ်ပါတယ်။ များစွာသော email ဖွံ့ဖြိုးရေးဝန်ဆောင်မှု အဖွဲ့တွေကတော့ ၎င်းတို့ software ရောင်းချသူများအပေါ်မူတည်၍ IMAP ပုံစံတစ်ခုခုကို အသုံးပြုကြပါတယ်။ IMAP မှာတော့၊ ခင်ဗျားရဲ့ စာတိုက်ပုံး (Mailbox)ထဲမှာ folder များတည်ဆောက်ခြင်း၊ အဲဒီ folder တစ်ခုမှ၊ တစ်ခုသို့ စာများလွှဲပြောင်းသိမ်းဆည်းနိုင်ခြင်းမှာ ပြုလုပ်နိုင်ပါတယ်။ ခင်ဗျားက IMAP server ကို ချိတ်ဆက်လိုက်တိုင်း၊ ခင်ဗျား Mailbox နှင့် server ကြားမှာ folder များ၊ ပါဝင်မှုများ၊ ရောက်ရှိလာသောစာများ နှင့် ပယ်ဖျက်ထားသောစာများ အပြန်အလှန် ချိတ်ဆက်ကြပါတယ်။ ၎င်း protocol မှာ ခင်ဗျားရဲ့ မည်သည့် ကွန်ပြူတာ၊ laptop၊ kiosk၊ phone နှင့် tablet တို့မှ မဆို ခင်ဗျား စာတွေကို ရယူနိုင်ခြင်းစတဲ့ ကောင်းကျိုးတော်တော်များများရှိပါတယ်။ ဒါ့အပြင် ၊ခင်ဗျားကိုယ်ပိုင် ကွန်ပြူတာပေါ်မှ ကိုယ်ရေးကိုယ်တာ အချက်အလက်ဖိုင်များထဲမှာလည်း ခင်ဗျားစာတွေကို သိမ်းဆည်းထားနိုင်ပါတယ်။

မည်သို့ဆိုစေ၊ ၎င်းမှာ ချွတ်ယွင်းချက် ၂ ချက် ရှိပါတယ်၊ ပထမတစ်ချက်အနေနဲ့ ခင်ဗျားအချက်အလက်များစွာ ပို့ဆောင်ရန် ပိုမိုမြန်ဆန်တဲ့ အင်တာနက်ချိတ်ဆက်မှုနှင့် အချိန်ပိုလိုအပ်တယ်ဆိုတာ၊ မြင်သာစွာသိနိုင်ပါတယ်။ ဒုတိယတစ်ချက်ကတော့ နေရာအကန့်အသတ်ရှိခြင်းပဲဖြစ်ပါတယ်။ ခင်ဗျား mail server ကခင်ဗျားအတွက် ကျော်သုံးလို့မရတဲ့ mailbox အရွယ်အစား တစ်ခုချမှတ်ပေးပါတယ်။ ကန့်သတ်မှုပြည့်သွားရင်တော့၊ ခင်ဗျားစာတွေမဖျက်ပစ်ပဲနဲ့(ဒါမှမဟုတ် နေရာထပ်မဝယ်ပဲနဲ့) ခင်ဗျား စာများကို ဆက်လက် လက်ခံရရှိနိုင်မှာမဟုတ်ပါဘူး။ ဤအချက်ကြောင့် အခြေခံအားဖြင့် IMAP email တွေက အချက်အလက် စီမံခန့်ခွဲမှုပြုလုပ်ရန် လိုအပ်ပါတယ်။ ခင်ဗျားmail တွေကို ခင်ဗျားကွန်ပြူတာပေါ်ရွှေ့ပြောင်းသိမ်းဆည်းရန်၊ ခင်ဗျားရဲ့ sent mail၊ spam mail တွေနှင့် trash တွေကို ပုံမှန်ရှင်းလင်းရန် လိုအပ်ပါတယ်။ attachments ပါတဲ့ mailတွေက ခင်ဗျားကို ဖျက်ဆီးနိုင်ပါတယ်။ ယဿုခေတ် ကြီးမားတဲ့ အခမဲ့ အချက်အလက်သိုလှောင်ရန်နေရာနှင့် အင်တာနက် email အကောင့်များအတွက်တော့၊ ထိုကဲ့သို့ ထိန်းသိမ်းမှုက၊ မိုက်မဲမှုပဲ ဖြစ်ပါလိမ့်မယ်။ ခင်ဗျားတရားဝင်သုံးစွဲရန်လိုလာတဲ့အထိ (သို့) တစ်စုံတစ်ယောက်က အဲဒီ mail server ကို ထိန်းချုပ်ပြီး ခင်ဗျား mail တွေ သိမ်းပိုက်လိုက်တဲ့အထိပေါ့။

POP server နှင့်၊ IMAP server နှစ်ခုစလုံးမှာ ခင်ဗျားအကောင့်ကို သုံးစွဲခွင့် ရနိုင်ရန် password တစ်ခုလိုပါတယ်။ ဒါပေမယ့်၊ အဲဒီ protocol နှစ်ခုစလုံးက password အပါဝင် မည်သည့်အရာမဆို ရှင်းလင်းစွာ သယ်ယူပို့ဆောင်ကြတာကြောင့်၊ ၎င်းတို့သယ်ယူပို့ဆောင်သမျှကို လူတိုင်းဖတ်ကောင်းဖတ်နိုင်နေပါလိမ့်မယ်။ ခင်ဗျားအနေနဲ့ ၎င်းတို့ကို ဖုံးကွယ်ပေးရန် (SSL)ကဲ့သို့ encryption ပုံစံအချို့ကို အသုံးပြုရန်လိုအပ်ပါတယ်။ ဒါကြောင့် email client တိုင်းလိုလိုမှာ၊ SSL အသုံးပြုရန် check box တစ်ခုပါဝင်လေ့ရှိတာ ဖြစ်ပါတယ်။

ခင်ဗျား email client က send ကိုနှိပ်လိုက်တာနဲ့၊ အကြောင်းအရာနှစ်ခုဖြစ်ပါတယ်၊ ပထမတစ်ခုက ခင်ဗျား client က ခင်ဗျားကို SMTP server (ခင်ဗျားက POP server ကို ချိတ်ဆက်ထားပြီးဖြစ်ရင်တောင်မှ) ကို ချိတ်ဆက်ရန် စကားပှက် ထည့်သွင်းဖို့ တိုက်တွန်းပါလိမ့်မယ်၊ ပြီးတော့မှ ခင်ဗျားရဲ့ အထွက်စာကို (outgoing mail) (SMTP protocol မှတဆင့်) ပို့ဆောင်ပေးပါလိမ့်မယ်။

ထိုအချက်က **POP-before-SMTP** လို့ခေါ်တဲ့ protocol ကို server များစတင်အသုံးပြုခဲ့တဲ့ အချိန်ဘဲ့၀ နှစ်လည်ပိုင်း ခန့်တွင်၊ ရှုပ်ထွေးစေခဲ့ပါတယ်။ **POP-before-SMTP** protocol က၊ ပထမဦးစွာ POP server ကို ခင်ဗျား user name နှင့် password ကိုဖြည့်သွင်းပြီး၊ အဝင်စာများကိုရယူပါတယ်၊ ထို့နောက်၊ SMTP server က POP server မှာခင်ဗျားအကြောင်းကို စစ်ဆေးပါတယ်၊ ("ဒီလူက မှန်ရဲ့လား?" "မှန်ပါတယ်၊ ငါသူကိုစစ်ဆေးပြီးပါပြီ") ပြီးတော့မှ ခင်ဗျားပို့လိုက်တဲ့စာတွေကို ပို့ဆောင်ပေးပါတယ်။ ၎င်းက တကယ်ကောင်းတဲ့ အချိန်ကိုက်ဝန်ဆောင်မှုပေးသူ (time-saver) တစ်ခုပါ။

သတိရရန် အရေးကြီးသောအချက်တစ်ခုက၊ စကားပှက်ကာထားရန်ဖြစ်သော်လည်း၊ email ကလျှိုပှက်အချက်အလက်တွေပေးပို့သင့်တဲ့ နည်းလမ်းတစ်ခုမဟုတ်ပါဘူး။ client နှင့် server အများစုက ခင်ဗျားရဲ့ စကားပှက်အား mail server ကိုချိတ်ဆက်ရန် encrypt မပြုလုပ်ထားရန်လိုအပ်ပါတယ်။ ခင်ဗျား mail ကိုရတဲ့သူတိုင်း ခင်ဗျား စကားပှက်ကို ရနေတယ်လို့တော့ မဆိုလိုပါဘူး ဒါပေမယ့်၊ ဗဟုသုတအားကောင်းသူတွေနဲ့ tools တွေကတော့ ခင်ဗျား စကားပှက်ကိုသာမက ခင်ဗျားmail တွေထဲမှ အကြောင်းအရာတော်တော်များများကို အနှံ့ခံနိုင်ပါတယ်။ (ခင်ဗျား email ကိုပိုမိုလုံခြုံစေရန် အကြံအဉာဏ်များကို **Lesson 9: Email လုံခြုံရေး အခန်းတွင် ဖတ်နိုင်ပါတယ်။**)

### လေ့ကျင့်ခန်းများ

4.5 ခင်ဗျား အဓိကသုံးတဲ့ email ကို အဲဒီ email မှပဲ စာပို့ကြည့်ပါ။ အဲဒီစာကိုပဲ အခြားအကောင့်မှ၊ ရှေ့မှပို့လိုက်တဲ့ email အကောင့်ကိုပဲ ထပ်ပို့ကြည့်ပါ၊ ဥပမာ- အခမဲ့ email အကောင့်တွေသုံးပြီးတော့ပေါ့ (လုပ်ပါ၊ ခင်ဗျားမှာရှိတာ ကျွန်တော်တို့သိပါတယ်)။ အဲဒီစာနှစ်စောင် ဘယ်စာကအရင်ရောက်သလဲ? အကယ်၍၊ ခြားနားမှုရှိရင် ဘာကြောင့် ဖြစ်ပါသလဲ?

4.6 ခင်ဗျား inbox ထဲမှာ ပိတ်မိနေတဲ့ သိန်းချီတဲ့ spam email များထဲမှ တစ်စောင်လောက်ဖွင့်ဖတ်ကြည့်ပါ။ အဲဒီစာတွေကို မည်သူကအမှန်တကယ်ပို့တယ်ဆိုတာ ခင်ဗျားဆုံးဖြတ်နိုင်ပါသလား? အဲဒီ emailတွေထဲမှာ ဟုက်ထားတဲ့ အချက်အလက်တွေများရှိနေမလား? ရှိနေတယ်ဆိုရင်၊ ပါးနပ်တဲ့ hacker တစ်ယောက်က ထိုကွယ်ဟုက်မှုတွေကို မည်သို့ ရှာတွေ့နိုင်ပါသလဲ?

4.7 ခင်ဗျား email တစ်ခုကို ပို့ရန် တိကျတဲ့အချိန် (သို့) နေ့အထိ ဆိုင်းငံ့ထားနိုင်ပါသလား (ထိုသို့ တကယ့်ကို တားဆီးထားနိုင်ပါသလား?)? ခင်ဗျားသူငယ်ချင်းတွေကိုလိုက်ရှုပ်ဖို့၊ email ပို့ခြင်းဆိုင်းငံ့မှုအသုံးပြုဖို့ နည်းလမ်းကောင်းများ ခင်ဗျား စဉ်းစားမိပါသလား?

## IRC

**IRC (inter Relay Chat)** ကတော့ ပြုပြင်ဖန်တီးထားခြင်းမရှိတဲ့ အင်တာနက်ရဲ့ အကောင်းဆုံးသဘာဝတရားကို သိမြင် နိုင်ရန်၊ အကောင်းဆုံးနေရာတစ်ခုပဲဖြစ်ပါတယ်။ ဒါမှမဟုတ် နံချာမှပေါ့။ IRC ပေါ်မှာ၊ လူတိုင်းပြောချင်ရာပြောနိုင်တယ်။ IRC ကို **သတင်းအုပ်စုများအဖွဲ့ (Usenet)** (သို့) **သတင်းအုပ်စုများ** ဟုခေါ်ပါတယ်။ သတင်းအုပ်စုတစ်ခုချင်းစီမှာ ကိုယ်ပိုင် နာမည်၊ နာမည်ခွဲ၊ နာမည်အခွဲများစွာ စသည်ဖြင့် ရှိကြပါတယ်။

chat roomတွေကိုတော့ ခင်ဗျားသိမှာပါ။ IRC က chat room တစ်ခုပဲဖြစ်ပါတယ်။ အဲဒီမှာ အခြေခံအားဖြင့် **အင်တာနက်သုံးသူများ လိုက်နာရမည့်ကျင့်ဝတ် (netiquette)** မှလွဲ၍ အခြားစည်းမျဉ်းများမရှိပါဘူး၊ ပြီးတော့ အဲဒီမှာကြီးကြပ်ရေးတွေလည်း မရှိပါဘူး။ အဲဒီမှာ ခင်ဗျားရှာဖွေနေတဲ့အရာကို ရှာတွေ့နိုင်သလို၊ ခင်ဗျားတစ်ခါမှ မသိခဲ့ဘူးတဲ့အရာတွေလည်း ရှာတွေ့နိုင်ပါတယ်။

> ခင်ဗျားကြားဖူးတဲ့ chat room တွေရဲ့ စည်းမျဉ်းအားလုံးက IRC channel များနှင့် သက်ဆိုင်ပါတယ်။ မည်သူကိုမျှ ခင်ဗျားနာမည်အမှန်မပြောပါနဲ့။ ခင်ဗျား ဖုန်းနံပါတ်၊ ခင်ဗျား လိပ်စာ (သို့) ခင်ဗျား ဘဏ်အကောင့် နံပါတ်တွေ မဖေါ်ပြပါနဲ့။ ဒါပေမယ့်၊ အပျော်ရှာပါ! အကယ်၍ခင်ဗျားက ခြေဦးတည့်ရာသွားနေရင်တော့၊ ရနိုင်တဲ့ အချက်အလက်တွေကို သတိပြုပါ။ အင်တာနက်ပေါ်ကရနိုင်သမျှတိုင်းက malware ကင်းမဲ့မှု မရှိနိုင်ပါဘူး၊ ပြီးတော့ အင်တာနက်ပေါ်က လူတိုင်းက လူကောင်းသူကောင်းတွေမဟုတ်ကြပါဘူး။

ခင်ဗျား စာရိုက်သမျှအားလုံးက IRC server များကြားမှာ ရှင်းလင်းသောစာသားများအဖြစ် ကူးသန်းသွားလာနေတာကြောင့် IRC ကလုံခြုံမှုမရှိပါဘူး။ ခင်ဗျား နှင့် အခြား IRC အသုံးပြုသူတစ်ဦးဦးကြားမှာ သီးသန့် စကားပိုင်းပြုလုပ်နိုင်ပါတယ်၊ ဒါပေမယ့် အဲဒီစကားပိုင်းကိုလည်း ရှင်းလင်းသောစာသားများအဖြစ် သာ ပို့ဆောင်ပါတယ်။ နာမည်ဟုက်အသုံးပြုခြင်းကသာ ခင်ဗျားကို လုံခြုံမှုနည်းနည်း ရှိစေနိုင်ပါတယ်။ အကယ်၍၊ ခင်ဗျားက ဖျက်လိုဖျက်ဆီးမှုတွေ၊ မသင့်လျော်မှုတွေပြုလုပ်ဖို့ ကြံစည်နေတာဆိုရင်တော့ အကောင့်အားလုံးအတွက် နာမည်ဟုက်တစ်ခုတည်းကိုပဲအသုံးမပြုပါနဲ့။ နာမည်ဟုက်တစ်ခုတည်းသုံးခြင်းက ခင်ဗျားကို အရမ်းတော်တဲ့လူတွေမပြောနဲ့ ရဲတွေတောင် ခြေရာခံမိနိုင်ဖို့ အကောင်းဆုံးနည်းလမ်းဖြစ်ပါတယ်။

အကြောင်းအရာတွေကို "channels" လို့ခေါ်ပါတယ်။ အဲဒီမှာ channel ပေါင်းများစွာရှိနေတာကြောင့်၊ ခင်ဗျားစိတ်ကုန်သွားတဲ့ အထိလေ့လာနိုင်ရန်၊ အဲဒီ IRC တွေစုစည်းထားတဲ့ URL တစ်ခု ပေးထားပါတယ်။

http://www.nic.funet.fi/~irc/channels.html

အကယ်၍၊ အခြားအသုံးပြုသူတွေရေးတဲ့၊ ပေဖန်ချက်တွေကြောင့် ပြဿဿနာရှိတယ်ဆိုရင်၊ (အကယ်၍ရှိခဲ့ရင်) moderator ကို သတင်းပေးတိုင်ကြားနိုင်သလို၊ အဲဒီလူကို၊ အဲဒီ channel မှ **တားမြစ် (bump)** လိုက်နိုင်ပါတယ်။ အကယ်၍ အသုံးပြုသူ တစ်ယောက်ယောက် ပြောချင်တာကို ခင်ဗျားမမြင်ချင်ဘူးဆိုရင်၊ သူတို့ကိုခင်ဗျား ဘလောခ့်ထားနိုင်ပါတယ် သို့မဟုတ် သူတို့ စာတွေကို ဥပကဿနာပြုထားနိုင်ပါတယ်။ ဒီလုပ်ငန်းစဉ်ကတော့ မည်သို့မျှ၊ ခင်ဗျားအတွက်မဖြစ်နိုင်ပါဘူး။

### လေ့ကျင့်ခန်းများ

4.8 security အကြောင်းအရာကို အဓိကပြောဆိုကြတဲ့ IRC channel ၃ ခုလောက်ရှာဖွေကြည့်ပါ။ အဲဒီထဲက အများဆိုင် စကားပိုင်းတွေကို မည်သို့ပါဂင်နိုင်ပါသလဲ? အဲဒီထဲက လူတစ်ယောက်ယောက်နှင့် သီးသန့်စကားပြောနိုင်ရန် မည်သို့ လုပ်ဆောင်နိုင်ပါသလဲ?

4.9 IRC က မည်သည့် port ကိုသုံးပါသလဲ?

4.10 IRC မှာ ဖိုင်တွေ ပို့ဆောင်လဲလှယ်နိုင်ပါသလား? မည်သို့လုပ်ဆောင်ပါသလဲ? ခင်ဗျားကရော IRC ကိုသုံးပြီး ဖိုင်တွေ အချက်အလက်တွေ ဖလှယ်ချင်ပါသလား?

4.11 မည်သည့်အရာက MIME နှင့် SMIME တို့ကြား အဓိက ကွာခြားချက်ဖြစ်ပါသလဲ? အတိုကောက်ဖော်ပြချက်တွေမှာ "S" က ခင်ဗျားအတွက် လုံခြုံမှု-Secure (အရိပ်အမြွက်) အလေးပေးသူကဲ့သို့ အရေးပါတဲ့အရာ ဖြစ်ပါသလား?

## FTP

သမားရိုးကျ **File Transfer Protocol (FTP)** တွေက ပုံမှန်အားဖြင့် port 20၊ 21 တွေမှာ လုပ်ငန်းဆောင်ရွက်ပါတယ်။ ၎င်းက ခင်ဗျားကို ကွန်ပြူတာနှစ်လုံးကြားမှာ ဖိုင်တွေပို့ဆောင်နိုင်ရန် ဆောင်ရွက်ပေးပါတယ်။ ၎င်းကို သီးသန့် ဖိုင်ပို့ဆောင်ရေး ကဲ့သို့ အသုံးပြုတဲ့အခါ၊ encryption နည်းလမ်းဖြင့် အလုပ်မလုပ်နိုင်တာကြောင့်၊ ၎င်း protocol ကို ဖိုင်များပို့ဆောင်ရန် အများအသုံးပြုနိုင်တဲ့ Linux distro အသစ်အတွက် ISO ကဲ့သို့ အမည်မသိ FTP server များအနေဖြင့် အခမဲ့ အသုံးပြုကြပါတယ်။

အမည်မသိ FTP တွေက ကွန်ပြူတာအသုံးပြုသူများအတွက် အင်တာနက်ပေါ်မှ ဖိုင်များဖလှယ်နိုင်တဲ့ အဓိကနည်းလမ်းဖြစ်ခဲ့ပါတယ်။ များစွာသော FTP server တွေကို ဖိုင်များ၊ ပရိဂရမ်များ တရားဂင် ဖြန့်ဝေရန် (၎င်းက ၂အခြေရှိ ကိန်းဂဏန်း ရောဂါများ ဖြန့်ဝေရန် အကောင်းဆုံးနည်းလမ်း) အသုံးပြုခဲ့ကြပါတယ်။ ပုံမှန် နည်းစနစ်ကိုသုံး၍ အမည်မသိ FTP ဂန်ဆောင်မှုများပေးနေတဲ့ server တွေကို ခင်ဗျားရှာတွေ့နိုင်ပါတယ်၊ ဥပမာအားဖြင့် search engine များပဲဖြစ်ပါတယ်။ ဒါပေမယ့် ကျွန်တော်တို့ user name နှင့် password များအကြောင်းပြောနေကြတာဆိုရင်တောင် FTP login တွေကို ရှင်းလင်းသောစာသားများဖြင့်သာ server သို့ ပို့ဆောင်တယ်ဆိုတာ မမေ့ပါနဲ့။ လုံခြုံတဲ့ FTP (SFTP) ရှိပေမယ့်၊ လူတိုင်းမသုံးကြပါဘူး၊ (ညံ့ဖျင်းလွန်းတယ် မဟုတ်လား?)။

FTP server တွေက web browser တစ်ခုကို ဖြတ်၍၊ FTP protocol ကိုသုံးလျက် ၎င်းတို့၏ ဖိုင်များကိုအသုံးပြုခွင့်ပြုပါတယ်။ ဖိုင်စီမံရေး ပရိဂရမ်တွေကဲ့သို့ အလုပ်လုပ်တဲ့ FTP client များလည်းရှိပါတယ်။ FTP server များကို၎င်းပြီး၊ ၎င်းပါမှ ဖိုင်တွေကို ခင်ဗျားကွန်ပြူတာပေါ်မှာဖိုင်ရွေးတဲ့ နည်းလမ်းအတိုင်းပဲ၊ ခင်ဗျားကွန်ပြူတာပေါ်သို့ ရွှေ့ပြောင်းနိုင်ပါတယ်။ FTP server တွေက အခြားတစ်နေရာမှာတည်ရှိနေနိုင်တာကြောင့် ခင်ဗျားကွန်ပြူတာပေါ်ဖိုင်တွေရောက်နိုင်ရန် အချိန်နည်းနည်းပိုကြာစေပါတယ်။

### လေ့ကျင့်ခန်းများ

4.12 Window, OSX နှင့် Linux များက များသောအားဖြင့် အခြေခံ FTP client command line များ ပါဂင်တတ်ပါတယ်၊ ၎င်းတို့ကို အသုံးပြုနိုင်ရန် terminal window (သို့) command prompt ကိုဖွင့်ပြီး အောက်ပါအတိုင်း ရိုက်ပါ။

```
ftp
```

ftp မှာ > help ရိုက်ပြီး၊ အသုံးပြုနိုင်တဲ့ command များရှာဖွေနိုင်ပါတယ်။

```
ftp > help
```

command များကို အကျဉ်းချုံးတွေ့နိုင်ပါတယ်။ command များကတော့ ။ ။

| | | | | |
|---|---|---|---|---|
| ! | delete | literal | prompt | send |
| ? | debug | ls | put | status |
| append | dir | mdelete | pwd | trace |
| ascii | disconnect | mdir | quit | type |
| bell | get | mget | quote | user |
| binary | glob | mkdir | recv | verbose |
| bye | hash | mls | remotehelp | |
| cd | help | mput | rename | |
| close | lcd | open | rmdir | |

**အခြေခံ command များ။ ။**

ftp server နာမည် ftp.domain.name: ကို ချိတ်ဆက်ပါ။

ftp > open ftp.domain.name

ၵင်း directory ထဲမှ ပါဂင်မှုတွေကို စီစစ်ပါ။

ftp> ls

(သို့)

ftp> dir

ၵင်း directory နာမည်ကို newdir လို့ပြောင်းပါ။

ftp> cd newdir

ၵင်း ကွန်ပြူတာထဲမှ ဖိုင်တစ်ခုကို ခင်ဗျားကွန်ပြူတာထဲသို့ ဒေါင်းလုပ်ယူပါ။

ftp> get filename

ၵင်း ကွန်ပြူတာထဲမှ ဖိုင်၂ခု၊ ၃ခု ခန့်လောက်ကို ခင်ဗျားကွန်ပြူတာထဲသို့ ဒေါင်းလုပ်ယူပါ (အဲဒီ directory ထဲမှ နောက်ဆက်တူ သောဖိုင်များစွာ (သို့) အားလုံး ကူးယူရန် wildcard များလည်း အသုံးပြုနိုင်ပါတယ်။)

ftp> mget file1 file2 file3

ခင်ဗျားကွန်ပြူတာမှ FTP ကွန်ပြူတာသို့ ဖိုင်တစ်ခုခု တင်ကြည့်ပါ။

ftp> put filename

FTP server နှင့် ချိတ်ဆက်မှုဖြတ်လိုက်ပါ။

ftp> close

ခင်ဗျား FTP client ကိုပိတ်လိုက်ပါ။

ftp> quit

**FTP** ကဏ္ဍသုတစ်ခု၊ အဆင့်လိုက်ဖေါ်ပြခြင်း

အမည်မသိ ftp ဂန်ဆောင်မှုတစ်ခုကို ချိတ်ဆက်အသုံးပြုရန်၊ ပထမဦးစွာ ခင်ဗျားရဲ့ စက်ပေါ်မှ FTP client ကို ဖွင့်လိုက်ပါ။

```
ftp
```

Server ကို ချိတ်ဆက်ရန် အဖွင့် command ကိုသုံးပါ။

```
ftp> open anon.server
```

anon.server နေရာမှာ၊ ဟုတ်ပါတယ်၊ တကယ့် server ရဲ့ နာမည်ကိုအစားထိုးပြီး ခင်ဗျားရဲ့ client ကို server နှင့် ချိတ်ဆက်လိုက်ပါ။

FTP server က ခင်ဗျားရဲ့ ချိတ်ဆက်မှုကိုလက်ခံလိုက်တဲ့အခါ၊ ခင်ဗျား client အား မိတ်ဆက်ပြီး ခင်ဗျားရဲ့ user name ကို တောင်းပါလိမ့်မယ်။

Connected to anon.server.

220 ProFTPD Server (Welcome . . . )

User (anon.server:(none)):

အမည်မသိ FTP server အများစုအတွက်ကတော့ user name မှာ anonymous (သို့) ftp ဟုဖြည့်သွင်းပေးရပါမယ်။ FTP server က ခင်ဗျားကို အမည်မသိ အသုံးပြုသူ အနေဖြင့် မှတ်တမ်းယူပြီး၊ password ထုတ်ပေးပါလိမ့်မယ်။

331 Anonymous login ok, send your complete email address as your password.

Password:

server အများစုက password အနေဖြင့် ခင်ဗျားဖြည့်သွင်းလိုက်တဲ့ email လိပ်စာကို မှန်၊ မမှန် မစစ်ဆေးတာကြောင့်၊ ခင်ဗျား email လိပ်စာမှားနေလည်း ခင်ဗျားကို အသုံးပြုခွင့်ရပ်ဆိုင်းလိုက်မှာမဟုတ်ပါဘူး။ ထိုအချက်ကို အင်တာနက် စီမံမှုတစ်ခု၏ ယိုစိမ့်ပေါက်အဖြစ် ထည့်သွင်းစဉ်းစားနိုင်သော်လည်း၊ မရှိမဖြစ်လိုအပ်တာကြောင့် email လိပ်စာအမှန်ကို မဖြည့်သွင်းသင့်ပါဘူး!။ ခင်ဗျား password တစ်ခု ထည့်သွင်းပြီးသည့်အခါ၊ ခင်ဗျားထံသို့ ကြိုဆိုခြင်း အကြောင်းကြားစာ ပို့ဆောင်ပါလိမ့်မယ်။

230-

Welcome to ftp.anon.server, the public ftp server of anon.server. We hope you find what you're looking for.

If you have any problems or questions, please send email to ftpadmin@anon.server

Thanks!

230 Anonymous access granted, restrictions apply.

ဒီကနေစပြီး၊ FTP server မှ ဖိုင်များရယူနိုင်ရန် ls, dir, cd, get စသည့် command များ စတင်အသုံးပြုနိုင်ပါပြီ။

### လေ့ကျင့်ခန်းများ

4.13 ဤဖေါ်ပြပါ ဥပမာများကို အသုံးပြု၍ အမည်မသိ FTP server တစ်ခုမှ ဖိုင်များရယူပါ။

4.14 ခင်ဗျား browser နှင့် search engine ကို သုံး၍ Alic in Wonderland ဝီဒီယိုပါဂင်တဲ့ အမည်မသိ FTP server တစ်ခုကိုရှာဖွေပါ ပြီးတော့ ftp client command line ကိုသုံး၍ ထိုဖိုင်ကို ခင်ဗျားကွန်ပြူတာပေါ်သို့ ရယူပါ၊ ခင်ဗျား browser ကို အသုံးမပြုပါနှင့်။

4.15 မည်သည့် FTP client တွေကပိုမိုကောင်းမွန်ပါသလဲ? ၎င်းတို့ command line အားလုံးကိုစုပြီး ခင်ဗျားအတွက် ကောင်းမွန်တဲ့ graphical interface ကို ရယူပေးပါသလား? Command line မှာအသုံးပြုနိုင်တာတွေကို graphical interface မှာ အသုံးပြုမရနိုင်တာမျိုးရှိပါသလား?

4.16 ခင်ဗျား ကွန်ပြူတာကရော FTP server တစ်လုံးအဖြစ် လုပ်ဆောင်နိုင်ပါသလား?

**Telnet and SSH**

**Telnet** ကိုသုံး၍ ခင်ဗျားအသုံးပြုနေသောကွန်ပြူတာမှ ခင်ဗျားအဝေးမှထိန်းနေသောကွန်ပြူတာထံ များစွာသော command များဖြင့်သွယ်နိုင်ပြီး၊ ခင်ဗျားကိုယ်တိုင် ထိုကွန်ပြူတာရှေ့မှာထိုင်၍အသုံးပြုနေသကဲ့သို့ ထိန်းချုပ်အသုံးပြုနိုင်ပါတယ်။ **Secure Shell (SSH)** ကတော့ telnet ၏ ရှင်းလင်းသောစာသားတွေကို လုံခြုံသော encrypt လုပ်ထားသောစာသားများဖြင့် အစား ထိုး၍ လုပ်ငန်းဆောင်ရွက်ပေးပါတယ်။

ထပ်ပြောပါမယ်၊ Windows, OSX နှင့် Linux တွေမှာ telnet client command လိုင်းတစ်ခု အခြေခံပါဝင်ပြီး၊ ၎င်းကို အသုံးပြုနိုင်ရန် command prompt (သို့) terminal window ကိုဖွင့်ပြီး၊ အောက်ပါအတိုင်း ရိုက်၍အသုံးပြုပါ။

telnet

telnet server ကို ချိတ်ဆက်နိုင်ရန်၊ ထို server အား ကြီးကြပ်သူက ခင်ဗျားအတွက်ပေးထားသော အကောင့်နှင့် စကားဝှက် လိုအပ်ပါတယ်၊ ဘာကြောင့်လဲဆိုတော့ telnet ပရိုဂရမ်ကိုသုံး၍ လုပ်ငန်းများစွာဆောင်ရွက်နိုင်ပြီး၊ ၎င်းတို့ထဲမှ အချို့အရာတွေကိုသုံးပြီး ထိန်းချုပ်နေသောကွန်ပြူတာကို သိမ်းပိုက်မှုပြုလုပ်နိုင်လို့ပါပဲ။

ယဿခုအချိန်အခါမှာ ကွန်ပြူတာအုပ်ချုပ်ရေးမှူးတွေက server တွေနဲ့ ကွန်ပြူတာအသုံးပြုသူတွေကို အဝေးတစ်နေရာမှ ကူညီထောက်ပံ့မှုပေးရန်ရည်ရွယ်၍ telnet ကို ပြန်လည်အသုံးပြုလာကြပါတယ်။ ၎င်းပဉန်ဆောင်မှုက အင်တာနက်စနစ်ဟောင်းရဲ့ အစိတ်အပိုင်းတစ်ခုဖြစ်ပြီး တွင်တွင်ကျယ်ကျယ်တော့ အသုံးမပြုကြပါဘူး။

Telnet ကိုသုံးပြီး၊ email ပို့ခြင်း၊ လက်ခံခြင်း နှင့် web စာမျက်နှာများ၏ source code များကြည့်ခြင်း (ထိုသို့လုပ်ငန်းများ ဆောင်ရွက်ရန် telnet က ခက်ခဲရှုပ်ထွေးသော်လည်း) များကဲ့သို့ အခြားသောလုပ်ငန်းတွေလည်း လုပ်ဆောင်နိုင်ပါတယ်။ ၎င်းအချက်တွေအားလုံးနီးပါးက တရားဝင်ဖြစ်ပါတယ်၊ ဒါပေမယ့်၊ ၎င်းတို့ကိုတလွဲအသုံးချပြီး၊ တရားမဝင်ကိစ္စသစတွေကိုလည်း လုပ်ဆောင်နိုင်ပါတယ်။ ခင်ဗျားအနေနဲ့၊ telent ကိုသုံးပြီး email တွေဖတ်တဲ့နေရာမှာ subject လိုင်းသာမက၊ ဒီစာကို ဒေါင်းလုတ် လုပ်မယ်၊မလုပ်ဘူး၊ ဖျက်မယ်၊မဖျက်ဘူးစသဖြင့် ဆုံးဖြတ်နိုင်ရန် စာကိုယ်၏လိုင်းအနည်းငယ်ကိုပါ ဖတ်ရှုနိုင်ပါ တယ်။

အကယ်၍ ခင်ဗျားက SSH ကိုသုံးမယ်ဆိုရင်တော့၊ လက်ရှိ ဗားရှင်းကိုအသုံးပြုရန်တော့ဂရုပြုပါ၊ ဘာကြောင့်လဲဆိုတော့ ဗားရှင်းအဟောင်းတွေမှာ အားနည်းချက်များစွာရှိပြီး များစွာသော အားနည်းချက်ရှာဖွေရေး ပရိုဂရမ်တွေက ထိုအားနည်းချက် တွေကို အင်တာနက်ပေါ်မှာလွယ်ကူစွာရှာဖွေနိုင်လို့ပါပဲ။

## ကစားပွဲစတင်ခြင်း : ငှဲကို command သုံးလိုက်ပါ

အဖိုးရဲ့မျက်မှန်ထူထူရှေ့ကအနက်ရောင်ဖန်သားပြင် မှာ စိတ်အားထက်သန်စွာခုန်ဆွဲဆွဲဖြစ်နေတဲ့ ညှို့နှိမ်ထားလေးတစ်ခုကဲ့သို့ မှိတ်တုတ်မှိတ်တုတ်လင်းလျက်ရှိတဲ့ အလင်းလေးက command တစ်ခုကို မျှော်လင့်နေပါတယ်။ တွန့်ရှုံ့နေတဲ့ ဦးခေါင်းပေါ်မှာ ပါးလွှာနေတဲ့မီးခိုးရောင်ဆံပင်တွေ၊ လေးတွဲစွာတဖျတ်ဖျတ်လွှင့်နေပြီး အဖိုးက သူ့ရဲ့ကီးဘုတ်ပေါ်မှာ စည်းချက်လိုက်နေခဲ့ပါတယ်။ Jace က အသံတိတ်စနဿဒရားဆရာရဲ့ တီးခတ်ဖျော်ဖြေမှုကို ထိုင်ကြည့်နေခဲ့ပါတယ်၊ တပ်၊ တပ်၊ တပ်၊ တပ်။ အဖိုးက jace ရဲ့နုပျိုတဲ့မျက်လုံးတွေကို ကြည့်ပြီးပြုံးပြလိုက်ပါတယ်။ ပြီးတော့၊ "Jace ရေ၊ မင်းကို ကမဿဘာအသစ်လေး တစ်ခုပြမလို့၊ မင်းရဲ့ ထိုင်ခုံခါးပတ်ကို သေချာပတ်ထားတော့နော်" လို့ပြောပြီး ရှုစ်နှစ်သမီးလေးကို မျက်လုံးတစ်ဖက်မှိတ် ပြလိုက်ပါတယ်။

Jace က အဖိုးရဲ့ကွန်ပြူတာခုံန ၁ း ရောက်ရုံလေးရှိသေးတယ်၊ သေတဿတာငယ်လေးထဲက တယ်လီဖုန်းမည်သံကိုကြားလိုက် ပါတယ်။ အဲဒီအဖြူရောင်သေတဿတာလေးက စွန့်ပစ်အမှိုက်ပုံးကမျိုချခံရတဲ့ ဘဲတစ်ကောင်ကဲ့သို့ အသံမျိုးပြောင်းသွားတဲ့အခါ အစိမ်းရောင်၊အနီရောင်မီးမျာ း လင်းလာပါတယ်။ အဖိုးက စိတ်အားထက်သန်နေတဲ့မျက်ခုံးတွေကိုပင့်လိုက်ပြီး သူ့ရှေ့က အနက်ရောင်ဖန်သားပြင်ပေါ်မှာ ဖြစ်နိုင်ချေရှိတဲ့ command

တွေနဲ့အစပြုလိုက်ပါတယ်။ ဘဲအော်သံ ရပ်ဆိုင်းသွားပြီး၊ တယ်လီဖုန်းသေတဿတာပေါ်မှ မီးများအားလုံး အစိမ်းရောင်ပြောင်းသွားပါတယ်။

"သတိထားနော်" လို့အဖိုးကပြောလိုက်ပါတယ်။

ပုံမှန်အားဖြင့် အဖိုးက "သတိထားနော်" လို့ ပြောလိုက်တာနဲ့၊ တစ်ခုခု ပေါက်ကွဲမှု (သို့) တစ်ခုခုဆီမှ မီးခိုးများထွက်လာတတ်ပါတယ်။ နောက်ပြီး "သတိထားနော်" ဆိုတာကို သူတစ်ခုခုအမှားလုပ်မိလို့ စိတ်ဆိုးလာတဲ့အခါမှာလည်း ပြောတတ်ပါသေးတယ်။ Jace ကတော့ ထိုစကားကို အမြဲကြားချင်နေတတ်ပါတယ်၊ ဘာကြောင့်လဲဆိုတော့ ထိုစကားက အံ့သြဖွယ်တစ်ခုခုမြင်တွေ့ဖို့ စိတ်လှုပ်ရှားစရာမျှော်လင့်ချက်ဖြစ်နေလို့ပါပဲ။

ကွန်ပြူတာ ဖန်သားပြင်၊ အိပ်မောကျနေရာမှ နိုးထလာခဲ့ပြီး၊ "Welcome to Cline's Bulletine Board System (BBS)." ဆိုတဲ့ ASCII နဖူးစည်းစာသားတစ်ခု ပေါ်လာခဲ့ပါတယ်။ "ငါတို့ အထဲရောက်ပြီပေ့ာ" လို့ အဖိုးက လက်ခုပ်တီးလျက်ပြောပြီး ရှစ်နှစ်သမီးလေး Jace ကိုလက်ဝါးရိုက်ဖို့ ကြိုးစားလိုက်ပါတယ်။ သူလက်တွေက သူမလက်နှင့် လက်မအနည်းငယ်လောက် လွဲချော်သွားပြီး ကလေးမရဲ့မျက်နှာကို ပုတ်မိသွားပါတယ်။ သူမကတော့ ရယ်မောနေပါတယ်။

သူတို့နှစ်ယောက်စလုံး ကွန်ပြူတာဖန်သားပြင်နှင့် ကီးဘုတ်ကိုပြန်ကြည့်လိုက်ပါတယ်။ ဘာဖြစ်လာမလဲဆိုတာကို ကြည့်နေရင်း အဖိုးကသူလက်ချောင်းတွေကိုပွတ်နေပြီး၊ Jace ကသူမရဲ့စိတ်ကူးတွေကိုပွတ်နေခဲ့ပါတယ်။ လမ်းပေါ်က အစာကိုစားတော့မယ့်လင်းတင့်ကဲ့သို့ အဖိုးက သူဦးခေါင်းကို ကီးတွေပေါ် ငုံထားပြီး command တွေကို စတင်ရိုက်နေခဲ့ပါတယ်။ ဦးခေါင်း မော့ကာ၊ ငုံကာနဲ့၊ ရိုက်နေရင်းက၊ အဲ ! လို့ပြောလျက် အဖိုးနောက်မှိထိုင်လိုက်ပါတယ်။ အဖိုး အရေးကြီးတာတစ်ခုခု မေ့နေပုံရပါတယ်။

ထိုနောက် ဆရာတစ်ယောက်ကဲ့သို့ လေသံနှင့် "Jace ရေ၊ ဒီမှာဘာဖြစ်နေတယ်ဆိုတာပြောဖို့ မေ့သွားတဲ့အတွက်အဖိုးတောင်းပန်ပါတယ်၊ အခု၊ အဖိုးတို့ တယ်လီဖုန်းလိုင်းပေါ်ကနေ နောက်ကွန်ပြူတာတစ်လုံးကို ချိတ်လိုက်တာပဲ။ အဲဒီက ဆူညံနေတဲ့တစ်ခုက "Modem" လို့ခေါ်တယ်၊ သူအလုပ်က ဒစ်ဂျစ်တယ်ကို အန်နလော့ဂ်၊ အန်နလော့ဂ်ကို ဒစ်ဂျစ်တယ်အပြန်အလှန်ပြောင်းပေးဖို့ပဲ။" လို့ပြောလိုက်ပါတယ်။ အဖိုးက တယ်လီဖုန်းစနစ်နဲ့ အခွင့်ရရင်၊ရသလို စမ်းသပ်ကစားနေတတ်တာကြောင့် Jace လည်း တော်တော်များများသိပြီးသားဖြစ်နေပါတယ်။ ပုံမှန်အသုံးပြုနေချိန်မှာ ၄၈ ဗို့အားရှိပြီး တယ်လီဖုန်းခေါ်ဆိုသံပေးနေချိန်မှာ ၉၀ ဗို့အားရှိတယ်ဆိုတာတွေကို၊ တယ်လီဖုန်း နည်းပညာရှင်တွေသိသင့်တာထက် သူမကပိုသိနေပါတယ်။ Plain Old Telephone Service သို့မဟုတ် POTS ဆိုတာ အဖိုးနဲ့ သူမအတွက်တော့ဟာသတစ်ခု ဖြစ်နေပါပြီ။ အဖွားကတော့ POTS ဆိုတဲ့ပျော်ရွှင်စရာဟာသအကြောင်းကို သိပုံမရပါဘူး။

စပ်စုတတ်သူတစ်ယောက် က တယ်လီဖုန်းလိုင်းတွေကိုကြားဖြတ်နားထောင်နိုင်ပါတယ်၊ ဒါပေမယ့် ထိုသို့နားထောင်နေတာကို ဗို့အားထိန်းညှိစက်သုံးပြီး ရှာဖွေသိရှိနိုင်ပါတယ်။ တစ်ယောက်ယောက်က ကြားဖြတ်နားထောင်နေတဲ့အခါ၊ တယ်လီဖုန်းလိုင်းဗို့အား က၊ ခဏလောက်ထိုးတက်သွားပြီး၊ အနည်းငယ်မြင့်တက်သွားတတ်ပါတယ်။ အဖိုးက၊ ဗို့အားညှိစက်မပါပဲ၊ ဘယ်မှမသွားလို့၊ ၎င်းကိုအဖွားထက်တောင်ပိုချစ်မယ်လို့ Jace က ထင်နေပါတယ်။ အခုအချိန်ထိ အဖိုးရဲ့စက်လေးကို "Valerie" ဗို့တိုင်းစက်လို့ နာမည်ပေးထားတုန်းပဲလေ။ အဲဒီစက်လေးက Jace ပြီးရင်၊ အဖိုးရဲ့ အကောင်းဆုံးမိတ်ဆွေပဲပေါ့။

Jace က စိတ်ပါယောင်ဆောင်နေတဲ့မျက်ဝန်းတွေနဲ့ အဖိုးကိုကြည့်နေပြီး အန်နလော့ဂ်မှ ဒစ်ဂျစ်တယ်ပြောင်းခြင်း၊ အသံလိုင်းမှ ဒစ်ဂျစ်တယ်လိုင်းသို့ပြောင်းခြင်း သင်ခန်းစာတွေပေါ်မှာ ပိုပြီးအာရုံစိုက်နေခဲ့ပါတယ်။ Modem လုပ်နိုင်တဲ့ အလုပ်တွေက၊ တော်တော်များပါတယ်။ အဖိုးက လေးကန်နေတဲ့ ကျောင်းသူကို သင်ခန်းစာဆက်လိုက်ပါတယ်၊ "အဖိုး ချိတ်ဆက်လိုက်တဲ့ ကွန်ပြူတာက၊ အခြားကွန်ပြူတာနဲ့ သူတို့ပေးသမျှဝန်ဆောင်မှုတွေကို အသုံးပြုခွင့်ပေးတယ်။" သူမတစ်ခါ မျှမကြားဖူးတဲ့ "ဝန်ဆောင်မှုများ" (services) ဆိုတဲ့အရာကို အခုကြားလိုက်ရပါတယ်။

"အဖိုး၊ ဝန်ဆောင်မှုတွေဆိုတာ ဘာပြောလိုက်တာလဲ?" သိချင်စိတ်ပြင်းပြတဲ့ကလေးမက အဆင်သင့်တဲ့အဖြေတစ်ခုကို မျှော်လင့်ပြီး၊ မေးခွန်းထုတ်လိုက်ပါတယ်။ "သိပ်ကောင်းတဲ့မေးခွန်းပဲ၊ မြေးချစ်လေးရေ၊ အဖိုးရဲ့ ကွန်ပြူတာကကွန်ယက်တစ်ခုထဲက ကွန်ပြူတာတွေနဲ့ချိတ်ဆက်လိုက်တာ၊ ဒါမှမဟုတ်၊ အဖိုးကွန်ပြူတာက ကမဿဘာကိုဖြတ်ပြီး၊ အခြားကွန်ပြူတာ ၁ တွေနဲ့ချိတ်ဆက်နိုင်ခွင့်ရသွားတာပေါ့၊ အဖိုးကိုအခြားကွန်ပြူတာတွေနဲ့ ချိတ်ဆက်ပြီး၊ ဖိုင်တွေယူသုံးနိုင်ဖို့၊ အချက်အလက် တွေရှာဖွေနိုင်ဖို့၊ လူတွေနဲ့စကားပြောဆိုနိုင်ဖို့ ပြီးတော့

အဲလိုအခုံဖွယ်အရာတွေလုပ်နိုင်ဖို့ ဒီ modem က၊ ကူညီပေးတယ် လေ။ အဲဒီကွန်ပြူတာတွေက File Transport Protocol, Usenet, IRC, Telnet နဲ့ Email တွေလို ဝန်ဆောင်မှုတွေကို လုပ်ဆောင်ပေးနေတာပေါ့။" လို့ ဝမ်းသာအားရပြန်ဖြေပေးလိုက်ပါတယ်။

Jace က အဲဒီအဖြေကို မကျေနပ်ပါဘူး၊ အဲဒီအဖြေကသူမအတွက် အခြားမေးခွန်းများစွာ တစ်ဟုန်ထိုး ပေါ်ထွက်လာစေပါတယ်။ အခု သူမက၊ မေးခွန်းကျည်ကပ်ကိုထည့်ပြီး၊ မောင်းတင်လိုက်ပြီး၊ အစုလိုက်အပြုံလိုက်ပစ်လွှတ်လိုက်ပါပြီ - "File Transfer Proto ဘာ? MIC ဆိုတာ? Telknit ကဘယ်ကလဲ? Imail က အထူးတံဆိပ်ခေါင်းသုံးလား? ဒီဂျစ်တယ်ကမဿဘာ ကဘာအရောင်လဲ? ဘယ်သူက Usednet ကိုတီထွင်လိုက်တာလဲ? အဖွားကရော အဲဒီဝန်ဆောင်မှုတွေကိုသုံးလား? ဘာလို့အဲဒါတွေကို ဝန်ဆောင်မှုတွေလို့ခေါ်တာလဲ? ကလေးတွေကရောဘယ်ကလာတာလဲ?"

အဖိုးက ပြင်းထန်တဲ့မေးခွန်းပစ်ချက်တွေကနေ၊ သူဦးနှောက်ကိုကာကွယ်ဖို့၊ နားကိုပိတ်ထားလိုက်ဖို့လိုနေပါပြီ။"ခဏလေး၊ ခဏလေး၊ ခဏလေး၊ ဖြေးဖြေးမေးပါ မြေးလေးရယ်။"

**ကစားပွဲ ပြီးဆုံးပါပြီ။**

## DNS

ခင်ဗျားသူငယ်ချင်း တစ်ယောက်ကို ဖုန်းခေါ်တဲ့အခါ၊ သူ့ရဲ့ ဖုန်းနံပါတ်အမှန်ကို သိဖို့လိုပါတယ်။ အဲလိုပဲ၊ အဝေးက ကွန်ပြူတာတစ်လုံးကိုချိတ်ဆက်ချင်တဲ့အခါ ၎င်းနံပါတ်ကိုလည်းသိဖို့လိုတာပေါ့။ ရှေ့မှာပြောခဲ့တဲ့သင်ခန်းစာကို ခင်ဗျားမှတ်မိမှာပါ အဲဒီမှာ အင်တာနက်ပေါ်က ကွန်ပြူတာတွေနဲ့၊ IP လိပ်စာတွေအကြောင်းပြောခဲ့ပါတယ်။

IP လိပ်စာတွေကို ကွန်ပြူတာတွေက ကောင်းကောင်းနားလည်ပေမယ့် လူတွေကတော့ နာမည်တွေကိုပဲမှတ်မိနိုင်ပါတယ်၊ **domain နာမည်တွေပေါ့။** ဥပမာ - Hacker Highschool website ကိုချိတ်ဆက်ရန် www.hackerhighschool.org လို့ web browser ရဲ့ address bar မှာ ရိုက်ရမှာပါ။ ဒါပေမယ့်၊ web browser တွေက Hacker Highschool website တင်ထားတဲ့ server ကိုခေါ်ရန်၊ နာမည်ကိုမသုံးပဲ IP လိပ်စာကိုသာ အသုံးပြုနိုင်ပါတယ်။ ခင်ဗျားကွန်ပြူတာမှာ domain နာမည်ကို IP လိပ်စာ အဖြစ်ဘာသာပြန်ပေးနိုင်ဖို့ အဓိပဿယပါယ်အချို့ ရှိကိုရှိရမှာပါ။ အင်တာနက်ပေါ်မှာ ကွန်ပြူတာပေါင်းရာချီ (သို့) ထောင်ချီ ရှိနိုင်တာကြောင့်၊ ခင်ဗျားကွန်ပြူတာပေါ်မှာ အဲဒီလိပ်စာတွေကိုရှာနိုင်ဖို့ စာရင်းဖိုင်တစ် ခု (**host ဖိုင်**) ရှိနေဖို့လိုပါလိမ့်မယ်။ ဘယ်လိုပဲဖြစ်ဖြစ်၊ တကယ်ဆို အင်တာနက်ပေါ်မှာ ကွန်ပြူတာတွေ သန်းနှင့်ချီရှိနေရုံမက၊ IP လိပ်စာတွေ နဲ့၊ domain နာမည်တွေ ကြားမှာ၊ အပြန်အလှန်ဆက်သွယ်မှု တွေကလည်း အဆက်မပြတ် ဖြစ်ပေါ်နေတာပါ။

**Domain Name Service (DNS)** ကိုတော့ domain နာမည်တွေကနေ၊ IP လိပ်စာတွေ (အပြန်အလှန်) အရှင်ထား၍ ဘာသာပြန်ရန် အသုံးပြုပါတယ်။ ခင်ဗျားက domain နာမည်တစ်ခု www.domainname.com လို့ web browser ရဲ့ address bar မှာ ရိုက်လိုက်တဲ့အခါ ခင်ဗျားရဲ့ web browser က ခင်ဗျားရဲ့ အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) က သတ်မှတ်ထားတဲ့ DNS server ကိုရှာဖွေချိတ်ဆက်ပါတယ်။ အကယ်၍ ၎င်း DNS server ရဲ့ database ထဲမှာ ခင်ဗျားခေါ်တဲ့ domain နာမည်ရှိနေရင် ၎င်းက ခင်ဗျားကွန်ပြူတာဆီကို IP လိပ်စာ ပြန်ပို့ပြီး ခင်ဗျားကို ဆက်ပေးမှာပါ။

တကယ်လို့ ခင်ဗျား DNS server ရဲ့ database ထဲမှာ www.domainname.com မရှိရင်တော့၊ ၎င်းက ခင်ဗျားရှာဖွေတဲ့ domain နှင့် ကိုက်ညီတဲ့ IP လိပ်စာကိုရှာတွေ့တဲ့အထိ ခင်ဗျားရဲ့တောင်းဆိုမှုကို အခြား DNS server တစ်လုံးမှ၊ တစ်လုံးလက်ဆင့်ကမ်းရှာဖွေပေးပါလိမ့်မယ်၊ (ရှာမတွေ့ရင်တော့) domain နာမည်ရှာမတွေ့ကြောင်း အကြောင်းပြန်ပေးပါလိမ့်။

### လေ့ကျင့်ခန်းများ

4.17 command line window ကိုဖွင့်ပြီး ခင်ဗျားကွန်ပြူတာရဲ့ IP လိပ်စာကို အတည်ပြုပါ။ မည်သည့် command ကို အသုံးပြုလိုက်ပါသလဲ? မည်သည့် IP လိပ်စာ တွေ့ရပါသလဲ?

4.18 ခင်ဗျားချိတ်ဆက်ထားတဲ့ DNS server ရဲ့ IP လိပ်စာကို အတည်ပြုပါ။ မည်သည့် command သုံးရပါသလဲ? ခင်ဗျားရဲ့ DNS လိပ်စာက ဘယ်လောက်ပါလဲ?

4.19 www.isecom.org ကို ping ကြည့်ပါ။ အဖြေတစ်ခုခု ရပါသလား? မည်သည့် IP လိပ်စာကို ping ကပြန်ပေးပါသလဲ?

4.20 ခင်ဗျားကွန်ပြူတာမှာ အခြား DNS တစ်ခုခုထည့်ပြီး တိုက်ရိုက်သုံးနိုင်ပါသလား? အကယ်၍၊ ရမယ်ထင်ရင် ခင်ဗျားကွန်ပြူတာမှာ အခြား DNS server လိပ်စာထည့်ပြီးသုံးကြည့်ပါ။ ပြီးတော့ www.isecom.org ကိုထပ် ping ကြည့်ပါ။ ရှေ့မှာရခဲ့တဲ့အတိုင်း တူညီတဲ့အကြောင်းပြန်မှုကိုရပါသလား? ဘာကြောင့် ရပါသလဲ?

## DHCP

**DHCP (သို့) Dynamic Host Configuration Protocol** ကို ကွန်ယက်တစ်ခုအတွင်းမှာရှိတဲ့ server တစ်လုံးမှ အဲဒီကွန်ယက်အတွင်းကို IP လိပ်စာတွေထုတ်ပေးနိုင်ရန်အတွက် အသုံးပြုပါတယ်။ အဲဒီ server မှာ အသုံးပြုရမည့် IP လိပ်စာများအတွဲလိုက် ထည့်သွင်းထားပါတယ်။ ကွန်ပြူတာတစ်လုံးက ၎င်းကွန်ယက်ကိုချိတ်ဆက်လိုက်တာနှင့်၊ IP လိပ်စာတစ်ခုရရှိနိုင်မှာဖြစ်ပါတယ်။ ကွန်ပြူတာတစ်လုံးလုံး အဲဒီကွန်ယက်အတွင်းမှထွက်သွားတာနှင့်၊ ထိုကွန်ပြူတာသုံးခဲ့တဲ့ IP လိပ်စာကို အခြားကွန်ပြူတာများရယူအသုံးပြုနိုင်ရန် နေရာလွတ်ဖြစ်သွားမှာပါ။

၎င်းက ကြီးမားတဲ့ကွန်ယက်တွေအတွက် တကယ်ကိုအသုံးဝင်ပါတယ်။ ကွန်ပြူတာတစ်လုံးချင်းစီကို လိုက်ပြီး ပုံသေ IP လိပ်စာပေးနေဖို့ မလိုတော့ဘူးပေါ့။ အဲဒီအစား DHCP server ကိုသုံးလိုက်နိုင်တာပေါ့၊ ကွန်ပြူတာအသစ်တစ်လုံး ကွန်ယက်တစ်ခုကို ချိတ်ဆက်တာနှင့်၊ ပထမဆုံးလုပ်ဆောင်တာက DHCP server မှ IP လိပ်စာတောင်းခံတာပါပဲ။ ၎င်းကွန်ပြူတာက IP လိပ်စာတစ်ခုရရှိသွားတဲ့အခါ၊ အဲဒီကွန်ယက်ထဲမှာရှိတဲ့ ပန်ဆောင်မှုအားလုံး သုံးနိုင်မှာဖြစ်ပါတယ်။

အခုပြောမှာကိုတွေးကြည့်ပါ။ wifi ကွန်ယက်အများစုမှာ DHCP ကိုဖွင့်ပေးထားပါတယ်၊ ဒီအချက်က၊ အဲဒီ subnet ထဲမှာရှိသမျှသူအားလုံး IP လိပ်စာတစ်ခုစီရနိုင်တယ်လို့ ဆိုလိုပါတယ်။ အကယ်၍၊ ခင်ဗျားက ကော်ဖီဆိုင်ဖွင့်နေတာဆိုရင်တော့ ဒါတကယ့်ကိုလိုအပ်ပါတယ်၊ ဒါပေမယ့်၊ ခင်ဗျားက လုံခြုံမှုရှိတဲ့ ရုံးတစ်ခုလုပ်နေတာဆိုရင်တော့၊ တိကျတဲ့ IP လိပ်စာသတ်သတ်မှတ်မှတ်ပေးရမှာပါ။ အခြေနေပေါ်မူတည်ပြီးလုပ်ရမှာပါ။

## ချိတ်ဆက်မှုများ

အရင်တုန်းကတော့၊ ကွန်ပြူတာတွေက modem တစ်ခုခုသုံးပြီး အင်တာနက်ကိုချိတ်ဆက်ပါတယ်။ Modem တွေက bit ကို အသံအဖြစ်၊ အသံကို bit အဖြစ်ပြောင်းပေးပါတယ်။ **mod**ulating၊ **dem**odulating လုပ်ဆောင်ပေးတာကြောင့်၊ modem လို့ ခေါ်တာပါ။ Modem အမြန်နှုန်းကို **baud** (တစ်စက္ကန့် မှာထုတ်လွှင့်ချက်တစ်ခုပြောင်းလဲကြိမ်နှုန်း) **နှင့် bps** (bits per second) ယူနစ်တို့ဖြင့် တိုင်းတာပါတယ်။ baud နှုန်းမြင့်ခြင်းက bps နှုန်းမြင့်ခြင်းကိုဆိုလိုပါတယ်၊ ဒါပေမယ့် ခင်ဗျားဘာလုပ်မှာလဲဆိုတာ ထည့်စဉ်းစားရမှာပါ။ ဗီဒီယိုထုတ်လွှင့်မှုတွေကဲ့သို့ bandwidth အသုံးများတဲ့ application တွေက၊ စွမ်းအားပြည့်တဲ့ကြီးတွေ (သို့) DSL ချိတ်ဆက်မှုတွေကို ပန်ပိစေခြင်းများရှိနေစဉ်မှာ၊ (ခင်ဗျား စာရိုက်နှုန်းမကောင်းခင်က အထောက်အကူပေးခဲ့တဲ့) နှစ် ၂၀ သက်တန်းရှိတဲ့ baud ၃၀၀ နှုန်း modem တွေအသုံးပြုနေဆဲဖြစ်လို့ ၎င်းတို့အတွက် **Multi-User Dungeons (MUDs)** ကို telnet ချိတ်သုံးနိုင်တဲ့ application များကဲ့သို့ application များရှိပါသေးတယ်။

## ISPs

ခင်ဗျားက အင်တာနက်ကို ခေါ်ကြည့်ရမှာမဟုတ်ပါဘူး၊ ခင်ဗျားကွန်ပြူတာကို အင်တာနက်ဆီချိတ်ဆက်ပေးမယ့် server ကို ချိတ်ဆက်မိဖို့ လိုတာပါ။ အဲဒီ server က အချိန်တိုင်း အလုပ်ပိနေပြီး၊ အမြဲဖွင့်ထားပါလိမ့်မယ်။ အဲဒီ server ကိုတော့ အင်တာနက်ပန်ဆောင်မှုပေးသူ (**Internet Service Provider (ISP)**) တစ်ဦးဦးက တည်ဆောက်တားတာဖြစ်ပါတယ်။

ISP တစ်ခုမှာ အဆက်မပြတ် တည်ရှိမှုသဘောရှိပြီး၊ ၎င်းမှာ ခင်ဗျားအသုံးပြုနိုင်တဲ့ ပန်ဆောင်မှုတွေ ပန်ဆောင်ပေးနေတဲ့ server များလည်းရှိပါတယ်။ ဒါပေမယ့် အဲဒီပန်ဆောင်မှုတွေကို ခင်ဗျားကိုယ်တိုင်လည်း ပန်ဆောင်မှုပေးနိုင်ပါတယ်။ ဥပမာ -

ခင်ဗျားကိုယ်ပိုင်ကွန်ပြူတာပေါ်မှာ email server တစ်ခု၊ တည်ဆောက်နိုင်ပါတယ်၊ ဒါပေမယ့် ၎င်း server အချိန်ပြည့်ဖွင့်ထားပြီး၊ အချက်အလက်တွေလွှဲပြောင်းပေးနိုင်ရန် အင်တာနက်နှင့် အမြဲချိတ်ဆက်ထားဖို့တော့လိုပါလိမ့်မယ်။ မည်သို့ဖြစ်စေ၊ mail server က အချိန်ပြည့် အလုပ်လုပ်နေတာကြောင့်၊ ISP တစ်ခုအနေနဲ့၊ များစွာသော အသုံးပြုသူများ၏ အကျိုးသက်ရောက်မှုကို ပိုမို၍ ခိုင်မာလာစေပါတယ်။ ISP ရဲ့ ကွန်ပြူတာများက **Network Access Point (NAP)** ကိုချိတ်ဆက်နိုင်ရန်၊ မြင့်မားတဲ့ အင်တာနက်ချိတ်ဆက်မှုကို အသုံးပြုပါတယ်။ အဲဒီ NAP တွေ **backbone** လို့ခေါ်တဲ့ အလွန်မြင့်မားတဲ့ချိတ်ဆက်မှုနှုန်း ပေါ် မှာ၊ အချင်းချင်း အတွင်းပိုင်းချိတ်ဆက်ခြင်းများပြုလုပ်ပါတယ်။ ထိုသို့ အရာများအတူတကွ လုပ်ငန်းဆောင်ရွက်နေခြင်းကိုပင် အင်တာနက်လို့ ခေါ်ပါတယ်။

## Plain Old Telephone Service

**Plain old telephone service (POTS)** ဆိုတာ၊ တစ်ချိန်က အင်တာနက်ချိတ်ဆက်ရန် တွင်ကျယ်စွာအသုံးပြုခဲ့တဲ့ နည်းပညာတစ်ခုပါ။ ၎င်း၏ အဓိကဆိုးဝါးမှုက အမြန်နှုန်းနှေးကွေးခြင်းပါပဲ ဒါပေမယ့်၊ ကိစ္စသစတော်တော်များများအတွက်တော့၊ ကျယ်ပြန့်စွာ၊ သုံးခဲ့ကြပါတယ်။ Intenet Service Provider အများစုမှာ၊ ပြည်တွင်းသုံးနံပါတ်တွေများစွာရှိတတ်ပြီး၊ လူတိုင်းလိုလိုမှာလည်း၊ ကြိုးဖုန်းလိုင်းတွေရှိကြပါတယ်။ သီအိုရီအရတော့၊ ခင်ဗျားမှာ modem တစ်လုံးနှင့်၊ ငွေအကြွေအပြည့်ရှိတယ်ဆိုရင်၊ မည်သည့် အများသုံးတယ်လီဖုန်းကမဆို (အခုခေတ်မှာ၊ ရှာတွေ့နိုင်သေးရင်ပေါ့) အင်တာနက်ချိတ်ဆက်နိုင်ပါတယ်။ ခင်ဗျားသုံးချင်တော့မှာတော့ မဟုတ်လောက်တော့ပါဘူး။

POTS က အရမ်းနှေးပါတယ်။ အမြန်ဆုံး တယ်လီဖုန်း modem တွေတောင် 56,600 bit per second (bps) ပဲရှိကြတယ်။ ဘာပဲဖြစ်ဖြစ်၊ သူတို့ရှင်းပြနေတာကြာညဉ့်ရတာတော့ အလိမ်အညာတစ်ခုလိုပါပဲ။ စွမ်းအားကန့်သတ်မှုကြောင့် အမှန်တကယ် ဒေါင်းလုပ်နှုန်းက၊ 53,000 bps ပဲရပြီး၊ သက်ရောက်မှုပမာနကလည်း အလွန်နိမ့်ပါတယ်။ ထိုအချက်က DSL (သို့) cable modem တွေနဲ့ လုံးဝမယှဉ်နိုင်ပါဘူး။

တယ်လီဖုန်း ဝန်ဆောင်မှုတွေ တွင်ကျယ်စွာရနိုင်တယ်၊ POTS အခြေခံတဲ့ ISP တွေက ဈေးပေါကြတယ် (တစ်ခါတစ်ရံဆို၊ အလကားနီးပါးပဲ)၊ ဒါတွေတော့အားသာတာပေါ့။ pirate လုပ်ထားတဲ့ဇာတ်ကားတွေကို၊ POTS ပေါ်ကနေ ကူးသန်းမှု မပြုလုပ်သင့်ပါဘူး၊ ဘာကြောင့်လဲဆိုတော့ ထိုအရာတွေက၊ မကောင်းမှုပါ၊ တရားမဝင်ကိစ္စသစတွေပါ ပြီးတော့၊ ထိုသို့လုပ်ခြင်းက၊ ခင်ဗျားရဲ့ ဖုန်းလိုင်းကို ညတိုင်း၊ ရက်သတ္တသတပါတ်တိုင်း ထိန်းချုပ်ထားမှာဖြစ်ပါတယ်။ ဒါပေမယ့် ခင်ဗျားအဖွားဆီကိုတော့၊ သတိရကြောင်း စာသား email တွေတော့ ပို့နိုင်ပါလိမ့်မယ်။ ဖုန်တက်နေတဲ့၊ DOS အခြေခံတဲ့ စက်ဟောင်းတစ်လုံးနဲ့တောင်၊ telnet ကိုသုံးပြီး email ပို့နိုင် သေးတာပဲ မဟုတ်လား။

## DSL

**Digital Subscriber Line (DSL)** ဆိုတာ၊ ပမာဏ ကြီးများတဲ့ အချက်အလက်တွေကို POTS အတွက်၊ တပ်ဆင်ထားတဲ့ ဂါယာကြိုးတွေပေါ်ကနေ ပို့ဆောင်တဲ့ နည်းလမ်းတစ်ခုပါ။ ၎င်းရဲ့ အဓိကအားသာချက်ကတော့၊ အန်နလောခ့် modem တွေ ထက်ပိုမိုမြန်ဆန်ပြီး၊ အမြဲတမ်းချိတ်ဆက်ထားနိုင်ပါတယ်။ ပြီးတော့၊ အင်တာနက်ကိုချိတ်ဆက်နေချိန်မှာလည်း၊ ဖုန်းခေါ်ဆို၊ လက်ခံခြင်း ပြုလုပ်နိုင်ပါတယ်။ အဓိက အားနည်းချက်ကတော့၊ ၎င်းရဲ့ စွမ်းဆောင်ရည်နှုန်းက၊ ခင်ဗျားက တယ်လီဖုန်းကုမ္ပဏီ နဲ့၊ အိတ်(စ)ချိန်းရုံးနှင့် နီး၊ မနီးပေါ်မူတည်ပါတယ်၊ အကယ်၍ ခင်ဗျားက အရမ်းဝေးတဲ့နေရာမှာ ရှိနေရင်တော့၊ ခင်ဗျားကံဆိုး တာပေါ့။

## Cable Modems

Cable Gateway တွေက၊ အင်တာနက်ချိတ်ဆက်ရန်၊ ပုံမှန် တယ်လီဖုန်းလိုင်းတွေကို အသုံးမပြုပါဘူး။ အဲဒီအစား၊ ကြိုးကုမ္ပဏီတွေက ထောက်ပံ့ပေးတဲ့ coaxial ကြိုးတွေကို သုံးကြတယ် (ဒါမှမဟုတ်၊ fiber-optic လိုင်းတွေပေါ့၊ ခင်ဗျားကံကောင်း ရင်ပေါ့)။ DSL တွေလိုပါပဲ၊ cable gateway တွေက အင်တာနက်ချိတ်ဆက်ထားချိန်မှာလည်း၊ ဖုန်းသုံးနိုင်တယ်၊ အမြဲတမ်း အင်တာနက် ချိတ်ထားနိုင်တယ်၊ ဒါပေမယ့် DSL ထက်တော့ပိုမြန်ပါတယ်။

Cable gateway တွေမှာ ယိုပေါက်အချို့တော့ရှိပါတယ်။ ပထမတစ်ခုက၊ cable gateway တွေကို ရှယ်ပြီးသုံးကြတာကြောင့်၊ ခင်ဗျား cable ပေါ်မှာ၊ ရှယ်ပြီးသုံးတဲ့လူများလာရင်၊ ခင်ဗျားလိုင်းနှေးသွားပါလိမ့်မယ်။ ဒုတိယတစ်ခုက၊ လိုအပ်တဲ့ ကြိုးပြေးဆွဲ

မှတွေကို ကြိုးကုမဿပဏီတွေက ပြုလုပ်ထားတဲ့နေရာတွေမှာသာ တပ်ဆင်အသုံးပြုနိုင်ပါလိမ့်မယ်။ အဆုံးဝါးဆုံးက၊ ခင်ဗျား ကြိုး လိုင်းပေါ်မှာ၊ သုံးလိုက်တဲ့ လမ်းကြောင်းတိုင်းကို၊ ခင်ဗျားကြိုးနဲ့ ရှယ်ယာသုံးနေတဲ့သူအားလုံး မြင်နေနိုင်တာပါပဲ။ ! တကယ်လို့၊ ခင်ဗျားကွန်ပြူတာကို၊ cable modem နဲ့ချိတ်ဆက်သုံးတယ်၊ ပြီးတော့ firewall မကာထားဘူး ဆိုရင်တော့၊ ခင်ဗျား အိမ်နီးချင်းတွေက ခင်ဗျားကွန်ပြူတာနဲ့ ဖိုင်အားလုံးကို မြင်နိုင်နေမှာပါ။ ခင်ဗျားရဲ့ဘဏ်အကောင့်ကို၊ အဲဒီနည်းနဲ့ တကယ် ရှယ်ပေးချင်သလား?

## Wimax

Wimax ဆိုတာ၊ DSL နှင့်ယှဉ်နိုင်တဲ့ ကြိုးမဲ့ဆက်သွယ်ရေးနည်းလမ်းတစ်ခု ဖြစ်ပါတယ်။ ဂါယာဆက်သွယ်ရေး စနစ်အသုံးပြုရန်၊ ဈေးကြီးလွန်းတဲ့၊ ခက်ခဲလွန်းတဲ့ နေရာတွေမှာ ၎င်းကိုအသုံးပြုပါတယ်။ signal အားနည်းခြင်း၊ များခြင်းကတော့ အဆောက်အဦးတွေ၊ သစ်ပင်နှင့် အခြားထုထည်ကြီးမားတဲ့ အရာတွေ ပေါ်မှာပဲမူတည်ပါတယ်။ အချို့က ပုံသေ access point တွေအနေ နဲ့ ဝန်ဆောင်မှုပေးပြီး၊ အချို့ ကျယ်ပြန့်တဲ့နေရာတွေမှာတော့ mobile access အနေနဲ့ အသုံးပြုနိုင်ပါတယ်။

## Wifi

Wifi ကတော့ ခင်ဗျား ISP ကိုချိတ်ဆက်ရန် နည်းလမ်းတစ်ခုတော့မဟုတ်ပါဘူး၊ ၎င်းက အိမ်မှာ၊ ကော်ဖီဆိုင်တွေ shopping mall တွေလို စီးပွားရေးလုပ်ငန်းတွေမှာ၊ အင်တာနက်ချိတ်ဆက်ရန်အသုံးပြုတဲ့ အခြေခံကွန်ယက်ချိတ်ဆက်မှု နည်းလမ်းတစ်ခုပါပဲ။ smart phone တွေနဲ့ laptop အားလုံးလိုလို wifi ကိုသုံးကြပါတယ်၊ ဒါကြောင့် wifi က attacker များအကြိုက်ဆုံး ပစ်မှတ်ဖြစ်နေတာပေါ့။ ခင်ဗျား အများသုံး wifi ကို သုံးနေတဲ့အခါ၊ ကိုယ့်ကိုယ်ကို လူထူတဲ့ အခန်းထဲမှာ ကိုယ်လုံးတီးနေနေရတယ်လို့ တွေးကြည့်ပါ၊ လူအားလုံးက ခင်ဗျားကိုဝိုင်းကြည့်နေကြတယ်လို့ယူဆပြီး၊ ကိုယ့်ကိုယ်ကို ကာကွယ်ပါ၊ ဘယ်သူမှမကြည့်နေနိုင်အောင် စီစဉ်ပါ၊ ဒါပေါ့၊ ခင်ဗျား ကြိုးမဲ့လုံခြုံရေးစနစ် သင်ခန်းစာကို ဖတ်တော့မှာပေါ့၊ မှန်တယ်ဟုတ်?

### လေ့ကျင့်ခန်းများ

4.21 ခင်ဗျားအိမ်မှာ၊ အင်တာနက်ရှိမယ်ဆိုရင်၊ ၎င်းက ဘာအမျိုးအစားလဲ? ခင်ဗျားဘယ်လိုပြောနိုင်တာလဲ?

4.22 ခင်ဗျား ကွန်ယက်အတွင်းမှာ၊ ဘယ်သူတွေကိုခင်ဗျားမြင်နေနိုင်လဲ? (ဘယ်လို ရှာတွေ့လိုက်တာလဲ?)

4.23 ခင်ဗျားချိတ်ဆက်မှုက အမြန်နှုန်းဘယ်လောက်လဲ? ခင်ဗျား ISP ကိုမဆက်သွယ်ပဲနဲ့ အမြန်နှုန်းကို မြှင့်နိုင်သလား?

4.24 ခင်ဗျား ISP ကဘယ်လို service တွေထပ်ပေးနိုင်လဲ? ကျွန်တော်တို့ services တွေအကြောင်းပြောခဲ့ပြီးပါပြီ၊

4.25 ခင်ဗျား ကွန်ပြူတာကနေ မည်သည့် service တွေပေးနိုင်ပါသလဲ?

### Feed Your Head: HTTP နှင့် ကစားခြင်း

HTTP ၊ Hypertex Transfer Protocol ၏အတိုကောက် အသုံးအနှုန်းပါ၊ ၎င်းက TCP/IP အဆင့်တွေရဲ့ ထိပ်ဆုံးမှာပါဝင်ပြီး၊ အောက်ဖေါ်ပြပါ၊ အဓိက RFC ၂ခု မှာပါဝင်ပါတယ်;

- (0.9 မှ အခြေခံတဲ့) 1.0 အတွက် 1945
- 1.1 အတွက် 2616

1.0 မှ 1.1 သို့၊ အဆင့်မြှင့်တဲ့အခါ၊ တိုးချဲ့နိုင်မှု၊ Caching ၊ Bandwidth ညှိနှိုင်းမှု၊ ကွန်ယက်ချိတ်ဆက်မှုစီမံရေး၊ စာပို့စနစ်၊ အင်တာနက်လိပ်စာ ဆက်သွယ်ရေး၊ error သတိပေးစနစ်၊ လုံခြုံရေး၊ တည်တံ့မှု နှင့် စစ်မှန်မှု စစ်ဆေးခြင်း၊ ပါဝင်မှု ဆွေးနွေးခြင်းများအတွက်၊ ကြီးမားတဲ့ ပြောင်းလဲမှုများ၊ အဆင့်မြင့်မှုများ ရှိပါတယ်။ 1.0 နှင့် 1.1 ကြား ကွာခြားမှုများက၊ web server တစ်ခုရဲ့ အချက်အလက်တွေ ရရှိနိုင်ရန် အလွန်အသုံးဝင်ပါတယ်။

အခြေခံအားဖြင့်၊ HTTP က သတ်မှတ်ချက်မဲ့ protocol တစ်ခုပါ။ Client တစ်ခုက Server ထံသို့၊ HTTP Request တစ်ခု ပို့တဲ့အခါ၊ server မှ HTTP Response တစ်ခု အကြောင်းပြန်ပါတယ်၊ Request/Response ပုံစံပေါ့။

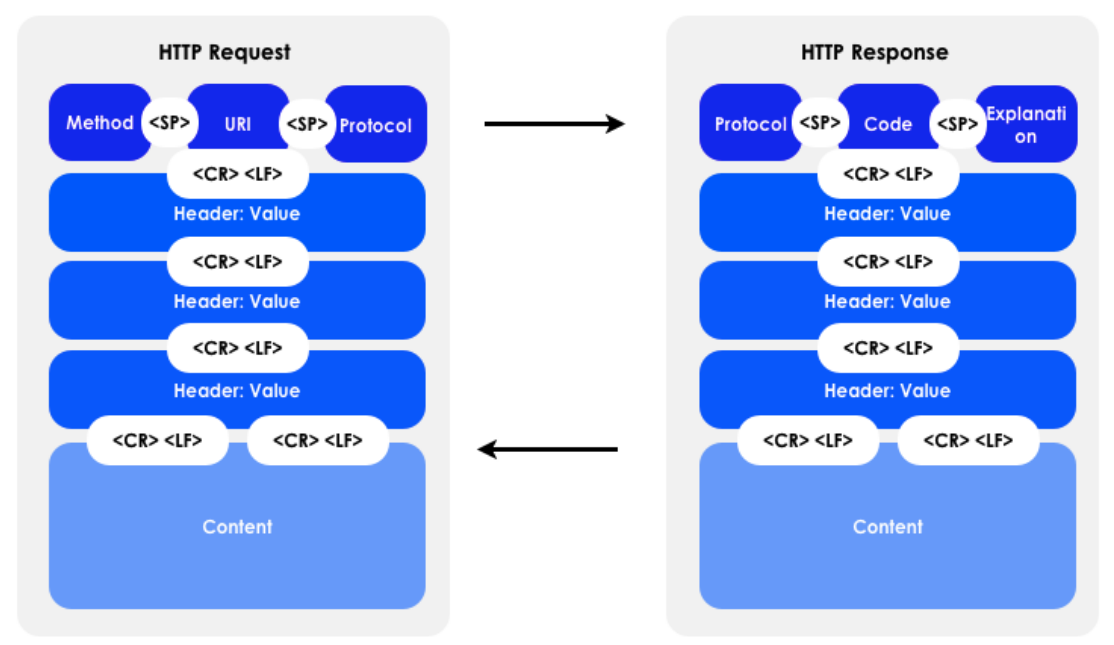


**Figure 4.1:** HTTP

HTTP server တစ်ခုဆီကို၊ command တွေရိုက်ပြီး၊ အချက်အလက်တွေရယူနိုင်တာ၊ ခင်ဗျားသိကောင်းသိပြီး ဖြစ်မှာပါ။ ကျွန်တော်တို့ အခြေခံ network tool လေးတွေသုံးကြည့်ရအောင်;

- netcat: the TCP/IP tool kit
- curl: the HTTP tool kit
- proxy: like OWASP ZAP or Burpsuite free

### ခင်ဗျားနဲ့ HHS ရဲ့ HTTP Server ကြားမှ ချိတ်ဆက်မှုကို အနံ့ခံ (Sniffing) လုပ်ကြည့်ပါ။

Proxy တစ်ခုခု သုံးပြီး၊ http://www.hackerhighschool.org ကိုချိတ်ဆက်ပြီး၊ ခင်ဗျား request ကို၊ ကြားဖြတ်ကြည့်ပါ။

GET / HTTP/1.1

Host: www.hackerhighschool.org

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:11.0) Gecko/20100101 Firefox/11.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip, deflate

Proxy-Connection: keep-alive

ပြီးတော့ အောက်ပါအတိုင်း response ပေးပါတယ်၊ ၊

HTTP/1.1 200 OK

Content-Length: 10376

Date: Fri, 03 Feb 2013 09:11:17 GMT

Server: Apache/2.2.22

Last-Modified: Mon, 06 Feb 2013 09:31:18 GMT

ETag: "2f42-4b8485316c580"

Accept-Ranges: bytes

Identity: The Institute for Security and Open Methodologies, The Institute for Security and Open Methodologies

P3P: Not supported at this time, Not supported at this time

Content-Type: text/html

Connection: keep-alive

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]><html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US" xml:lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><title>Hacker Highschool - Security Awareness for Teens</title>

[...]

**လေ့ကျင့်ခန်းများ**

4.26 ဖေါ်ပြပါပုံကို သုံးပြီး၊ proxy မှပို့တဲ့ request ကို စစ်ဆေးကြည့်ပါ။

4.27 Header မှာ စိတ်ဝင်စားစရာတွေ့ပါသလား?

**ခင်ဗျားရဲ့ ပထမဆုံး ကိုယ်တိုင်ချိတ်ဆက်မှု**

host port ကိုသုံး၍၊ web server အားချိတ်ဆက်ရန် Netcat ကို အသုံးပြုနိုင်ပါတယ်။

ယဉ်သခုလိုရိုက်ပြီး စတင်လိုက်ပါ။ ။

nc www.hackerhighschool.org 80

Enter နှစ်ကြိမ်ခေါက်လိုက်ပါ။

GET / HTTP/1.0

အောက်ဖေါ်ပြပါအတိုင်း server မှ အကြောင်းပြန်ပါလိမ့်မယ်:

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]>

<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US" xml:lang="en"><head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>ISECOM - Institute for Security and Open Methodologies</title> <meta name="description" content="Description" />

ခင်ဗျားတွေ့တဲ့အတိုင်းပဲ၊ hackerhighschool.org စာမျက်နှာပေါ်မလာပဲ၊ isecom.org စာမျက်နှာပေါ်လာပါဘယ်၊ ဘာလို့ပါလဲ?

ဖြစ်နိုင်တဲ့ အယူအဆတစ်ခုက၊ host server တစ်ခုတည်းမှာ၊ HHS ရော၊ ISECOM ပါ တင်ထားတာဖြစ်နိုင်ပါသလား?

hackerhigherschool.org IP လိပ်စာကို စစ်ကြည့်ရအောင်။

nslookup www.hackerhighschool.org

[...]

Non-authoritative answer:

www.hackerhighschool.org canonical name = hackerhighschool.org.

Name: hackerhighschool.org

Address: 216.92.116.13

အခု www.isecom.org ကို စစ်ကြည့်ရအောင် ။ ။

nslookup isecom.org

[...]

Non-authoritative answer:

Name: isecom.org

Address: 216.92.116.13

IP လိပ်စာ တူညီနေပါတယ်! ဒါဆို၊ ၎င်း host ရဲ့ HTTP 1.1 ကို manual ရိုက်ထည့်၍၊ Netcat ကိုသုံးခြင်းကသာ၊ Host header ကို ထုတ်ပြနိုင်ပါလိမ့်မယ်။

GET / HTTP/1.1

Host: www.hackerhighschool.org

HTTP/1.1 200 OK

Content-Length: 10376

Date: Fri, 03 Feb 2013 09:11:17 GMT

Server: Apache/2.2.22

Last-Modified: Mon, 06 Feb 2013 09:31:18 GMT

ETag: "2f42-4b8485316c580"

Accept-Ranges: bytes

Identity: The Institute for Security and Open Methodologies, The Institute for Security and Open Methodologies

P3P: Not supported at this time, Not supported at this time

Content-Type: text/html

Connection: keep-alive

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]>

<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US" xml:lang="en"><head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Hacker Highschool - Security Awareness for Teens</title>

## The Request Method

HTTP request တစ်ခု၏ ပြောင်းလဲပြင်ဆင်နိုင်တဲ့ အခြားအစိတ်အပိုင်းကို၊ Request Method လို့ခေါ်ပါတယ်။ ထုံးစံအားဖြင့်၊ web application တွေမှာ GET နှင့် POST request တွေကို သုံးကြပေမယ့်၊ အခြား request protocol တွေလည်း၊ web server (သို့) web application server တွေမှာ အလုပ်လုပ်ပါလိမ့်မယ်။ ဘုံသုံးဖြစ်တဲ့ နည်းလမ်းတွေကတော့ ။ ။

- **OPTIONS** – ကို မည်သည့် request တွေ အသုံးပြုနိုင်သလဲဆိုတာ၊ ရှာဖွေရန် အသုံးပြုပါတယ်။ အကယ်၍ ခင်ဗျားက web server တစ်လုံး၊ ပြုလုပ်ထားတယ်ဆိုရင် အချက်အလက်တွေ ဤနည်းဖြင့် ပေါက်ကြားနိုင်ခြင်းက ပြဿသသသနာတစ်ခုဖြစ်လို့၊ သေချာစွာသတိပြုပါ။

- **GET** – ကို URL မှ အချက်အလက်တွေ၊ တိုက်ရိုက်ယူရန် အသုံးပြုပါတယ်၊ ဥပမာ ။ ။
http://www.usairnet.com/cgi-bin/launch/code.cgi?Submit=Go&sta=KSAF&state=NM

  question mark နောက်မှတွေ့ရတဲ့ အရာအားလုံးကို တွေ့တယ်မဟုတ်လား? ၎င်းက request အချက်အလက်တွေပါ။ အချက်အလက်တွေကို ဤနည်းနဲ့ပေးပို့ခြင်းက၊ လွယ်ကူစွာတွေ့မြင်နိုင်လို့၊ စွန့်စားလွန်းရာကျပါတယ်။

- **HEAD** – ကို GET ကဲ့သို့အသုံးပြုပါတယ်၊ ဒါပေမယ့် server က စာမျက်နှာအမှန်ကို ပြန်ထုတ်မပေးပါဘူး။ ၎င်းကို အသုံးပြုခွင့်တွေ စစ်ဆေးရန်၊ bandwidth အသုံးပြုမှုတွေ ညှိနှိုင်းရန်၊ အချို့ ကိစ္စသစတွေမှာ ၊ အသုံးပြုခွင့် ထိန်းချုပ်မှုတွေကို ကျော်လွှားရန်အတွက် အသုံးပြုပါတယ်။ အမှန်တော့ အချို့ ACL အကောင်အထည်ဖော်ခြင်းတွေက GET request တစ်ခုတည်းကို စစ်ဆေးပါတယ်။ ဤအချက်မှ အားနည်းချက်တစ်ခုခု ရှာတွေ့နိုင်ပါတယ်။

- **POST** – ကို web application ဆီသို့ အချက်အလက်တွေပေးပို့ရန် အသုံးပြုပါတယ်၊ GET လိုပါပဲ၊ ဒါပေမယ့် အချက်အလက်တွေကို Request Body မှာ ပြောင်းရွေ့ပါတယ်။

- **PUT** – ကိုတော့၊ web server ပေါ်မှ အရင်းမြစ်တွေ ခွဲဝေသတ်မှတ်ရန် (သို့) ၎င်းကို အဆင့်မြှင့်ပေးရန် အတွက် အသုံးပြုပါတယ်။ context အများစုမှာ ဤနည်းလမ်းကို ပိတ်ထားသင့်ပါတယ်၊ ဒါမှမဟုတ်၊ အထောက်အထားစစ်ဆေးခြင်းဖြင့်၊ ကာကွယ်ထားသင့်ပါတယ်။ အခြား context များမှာ ၎င်းကို၊ နှစ်လိုဖွယ်တွေ့နိုင်ပါတယ်။

- **DELETE** – web server တစ်ခုပေါ်မှာ အရင်းမြစ်များနေရာလွတ်စေရန် အသုံးပြုပါတယ်။ ဤနည်းလမ်းကိုလည်း

ပိတ်ထားခြင်း၊ ကာကွယ်ထားခြင်းများပြုလုပ်သင့်ပါတယ်။

- **TRACE** – သတင်းများကို သုံးသပ်ပေးတဲ့၊ application layer loopback တစ်ခုကဲ့သို့ အသုံးပြုပါတယ်။ ၎င်းက၊ လျှို့ဝှက်ချက်တစ်ခုဖြစ်ပြီး၊ Cross Site Scripting တိုက်ခိုက်မှုတွေအတွက် အသုံးပြုနိုင်တဲ့၊ အားနည်းချက်တစ်ခုခုကို ဖြစ်စေတာကြောင့်၊ ဤ debug နည်းလမ်းကို အထူးသဖြင့် ထုတ်လုပ်မှုပိုင်းမှာ ပိတ်ထားသင့်ပါတယ်။

- **CONNECT** – ကို web server တစ်ခုအား proxy တစ်ခုကဲ့သို့ သုံးရန်အသုံးပြုပါတယ်။ ၎င်းက အသုံးပြုသူတွေ ကို proxy IP မှတဆင့် third party ဝန်ဆောင်မှုတွေကိုချိတ်ဆက်ခွင့်ပေးနိုင်တာကြောင့်၊ အထောက်အထားစစ်ဆေး ခြင်းဖြင့်၊ ကာကွယ်ထားသင့်ပါတယ်။

HTTP ပေါ်အခြေခံတဲ့ protocol များက WebDAV ကဲ့သို့ နည်းလမ်းများ ထည့်သွင်းနိုင်တယ်ဆိုတာလည်း စဉ်းစားဖို့ လိုပါတယ်။ ခင်ဗျားအနေနဲ့ server များမှ စိတ်ဝင်စားစရာအရာတွေ၊ နည်းလမ်းတွေသိရှိနိုင်ရန်နှင့် ခင်ဗျား စိတ်ထင်ရာ စကားလုံးတွေ စတဲ့အချက်များ ရရှိနိုင်ရန် Request Method ကို၊ ပြောင်းလဲအသုံးပြုနိုင်ပါတယ်။

**Requesting OPTIONS**

ပုံမှန်အနေနဲ့၊ netcat နဲ့ပဲ အစပြုပါ။

# nc www.hackerhighschool.org 80

ဒီတစ်ခါတော့ Enter ၂ကြိမ်မခေါက်ပါနဲ့၊ အဲဒီအစား next line မှာပဲ ရိုက်ကြည့်ပါ။

OPTIONS / HTTP/1.1

ပြီးတော့ ယဿခုလို response တွေရပါလိမ့်မယ် ။ ။

Host: www.hackerhighschool.org

HTTP/1.0 200 OK

Date: Tue, 07 Feb 2013 08:43:38 GMT

Server: Apache/2.2.22

Allow: GET,HEAD,POST,OPTIONS

Identity: The Institute for Security and Open Methodologies, The Institute for Security and Open Methodologies

P3P: Not supported at this time, Not supported at this time

Content-Length: 0

Content-Type: text/html

**Requesting HEAD**

ဒီတစ်ခါ HEAD option ကိုထည့်သွင်းလိုက်ပါ။

```
# nc www.hackerhighschool.org 80
HEAD / HTTP/1.1
```

```
Host: www.hackerhighschool.org

HTTP/1.0 200 OK
Date: Tue, 07 Feb 2013 08:41:14 GMT
Server: Apache/2.2.22
Last-Modified: Fri, 13 Feb 2013 15:48:14 GMT
ETag: "3e3a-4bd916679ab80"
Accept-Ranges: bytes
Content-Length: 15930
Identity: The Institute for Security and Open Methodologies
P3P: Not supported at this time
Content-Type: text/html
Age: 45
Connection: close
```

**ကဲ ခင်ဗျားကို Proxy တစ်ခုအနေနဲ့ ကျွန်တော်သုံးတော့မယ်နော်။ ။ the CONNECT Request**

# nc www.hackerhighschool.org 80

CONNECT http://www.isecom.org/ HTTP/1.1

Host: www.hackerhighschool.org

**လေ့ကျင့်ခန်းများ**

4.28 Netcat (nc) ကို သုံးပြီး အပေါ်မှာပြောခဲ့တဲ့ Request method တွေအားလုံးကို HHS network server ပေါ်မှာ စမ်းသပ်ကြည့်ပါ။ မည်ကဲ့သို့ စိတ်ဝင်စားစရာကောင်းတဲ့အရာတွေ ခင်ဗျားတူးဆွနိုင်ပါသလဲ?

## Curl ဖြင့် HTTP request တွေ script ရေးခြင်း

အခု web application စမ်းသပ်ချက်တွေက၊ web server response ပေါ်မှာပါမက၊ (Web) application အလွှာပေါ်မှာ ပါ အခြေခံပါတယ်။ GET နှင့် POST တွေ cookies နှင့် header များကို ပြင်ဆင်အသုံးပြုပြီး web application အားနည်း ချက်တွေ ရှာတွေ့နိုင်ပါတယ်။ bash scripting အတွက် အသုံးဝင်တဲ့ tool တစ်ခုကတော့၊ web page တစ်ခုကို request လုပ်ရန်သုံးတဲ့ **curl** command ပဲဖြစ်ပါတယ်။ ဒါပေမယ့် curl က netcat ပေါ်မှာ logic တစ်ချို့ကို ထည့်သွင်းထားတာ ပါ။

မေးကြည့်ရအောင် ။ ။

# curl http://www.isecom.org

nc နဲ့ မတူပါဘူး။ ။

# nc www.isecom.org 80

GET / HTTP/1.1

-v switch ကိုသုံးပြီး verbos (အပြည့်အစုံ) ရလာဒ်ကို ကြည့်နိုင်ပါတယ်။

```
# curl -v http://www.isecom.org/
* About to connect() to www.isecom.org port 80 (#0)
*   Trying 216.92.116.13...
* connected
* Connected to www.isecom.org (216.92.116.13) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.isecom.org
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Date: Tue, 07 Feb 2013 09:29:23 GMT
< Server: Apache/2.2.22
< Last-Modified: Fri, 13 Feb 2013 15:48:14 GMT
< ETag: "3e3a-4bd916679ab80"
< Accept-Ranges: bytes
< Content-Length: 15930
< Identity: The Institute for Security and Open Methodologies
< P3P: Not supported at this time
< Content-Type: text/html
< Age: 247
< Connection: close
<
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"[]>
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US" xml:lang="en">
[...]
```

အခုခင်ဗျားတွေ့တဲ့အတိုင်းပဲ၊ curl က HTTP version 1.1 ကို အလိုလျောက်ရွေးချယ်ပေးပြီး host header ၊ user agent တွေကို ထည့်သွင်းဖော်ပြပါတယ်။ hacker တွေအတွက် အရေးကြီးတာတစ်ခုက ဘယ်အချက်တွေလဲ ။ ။ ခင်ဗျားသုံးရမယ့် tool တွေကို သိအောင်လုပ်ပါ။

ကံကောင်းစွာနဲ့ curl က switch တွေကို သုံးပြီး၊ လိုသလိုပြင်ဆင်နိုင်တဲ့ tool ကောင်းတစ်ခုဖြစ်နေပါတယ်။

curl -help switch တွေကို လေ့လာကြည့်ပါ။ အချို switch တွေက netcat ဥပမာနှင့် ဆင်တူပါတယ်။

- **-H** header line ထည့်သွင်းရန်
- **-X** request method ရွေးချယ်ရန် (Command လိုလည်းသိနိုင်ပါတယ်)
- **-d** POST ထည့်သွင်းရန်
- **-i** protocol header များရလာဒ်တွင်ပါဝင်စေရန်
- **-s** scripting အတွက်အသုံးဝင်တဲ့ silent mode အသုံးပြုရန်

curl နှင့် အချို bash script တွေကို သုံးပြီး web application testing တွေ ဖန်တီးနိုင်ပါတယ်။ curl နှင့် grep ကို အတူတွဲ၍ သုံးပြီး server တစ်ခုမှ စိတ်ဝင်စားစရာ HTTP header တွေရှာဖွေခြင်းများပြုလုပ်နိုင်ပါတယ်။

```
# curl -siX HEAD http://www.isecom.org/ | grep "Server:"
Server: Apache/2.2.22
```

### လေ့ကျင့်ခန်းများ

4.29 အပေါ်က script တွေကို HTTP header တွေ အသုံးဝင်နိုင်ခြေရှိတဲ့ အချက်အလက်တွေ ပိုမိုရရှိရန် ချဲ့ထွင် အသုံးပြုပါ။

### ပိုမိုဖတ်ရှုရန်၊ အထောက်အပံ့ပေးနိုင်တဲ့ လင့်ခ်များ

http://www.ietf.org/rfc/rfc1945.txt

http://www.ietf.org/rfc/rfc2616.txt

http://www8.org/w8-papers/5c-protocols/key/key.html

http://netcat.sourceforge.net/

http://curl.haxx.se/

## အနှစ်ချုပ်များ

World Wide Web ဆိုတာ အင်တာနက်ထက် အများကြီးပိုပါတယ်။ ။ အဲဒီမှာ HTTP, FTP, SSH, DNS, DHCP နှင့် ခင်ဗျားနှင့် အခြားလူများ ရဲ့ ကွန်ပြူတာတွေအတွက် ဂန်ဆောင်ပေးနေတဲ့ ဂန်ဆောင်မှုတွေအပြင် အခြားများစွာသော ဂန်ဆောင်မှုတွေ လည်းရှိပါသေးတယ်။ အဲဒီ ဂန်ဆောင်မှုတွေကို "သင့်လျော်သော ကဏ္ဍသုခ" တွေ့ အသုံးပြု၍ဖြစ်စေ၊ အခြားနည်းလမ်းဖြင့်ဖြစ်စေ၊ ဘယ်လိုချိတ်ဆက်သုံးရမလဲဆိုတာ နားလည်ခြင်းက ခင်ဗျား (သို့) ခင်ဗျားကွန်ပြူတာကို မည်သို့ တိုက်ခိုက်ခံရနိုင်တယ်ဆိုတာ သိနိုင်ရန် သော့ချက်ပဲဖြစ်ပါတယ်။ ဤဆောင်ပုဒ်ကိုအမြဲသတိရပါ "Hack everything, but harm none".

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

**The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.**

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

**The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.**

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM